PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-106148
(43)Date of publication of application : 24.04.1998

(51)Int.Cl. G11B 20/10
G06F 12/14
G09C 1/00
H04L 9/08

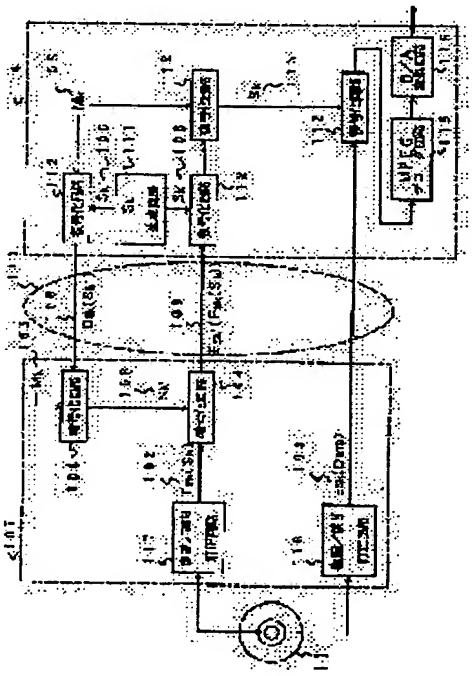
(21)Application number : 09-136709
(22)Date of filing : 27.05.1997

(71)Applicant : TOSHIBA CORP
(72)Inventor : KATO TAKEHISA
ENDO NAOKI
UNNO HIROAKI
KOJIMA TADASHI
HIRAYAMA KOICHI

(30)Priority
Priority number : 08170399 Priority date : 28.06.1996 Priority country : JP

(54) CIPHERING METHOD, DECODING METHOD, RECORDING AND REPRODUCING DEVICE, DECODING DEVICE, DECODING UNIT DEVICE, RECORDING MEDIUM, MANUFACTURE OF RECORDING MEDIUM AND METHOD OF MANAGING KEY

(57)Abstract:
PROBLEM TO BE SOLVED: To protect a copyright from piracy in preventing illegal copies by ciphering a data with a 1st key and ciphering this 1st key with predetermined plural 2nd keys.
SOLUTION: A 2nd session key Sk' is generated by a session key generating circuit 111, and is decoded by a decoding circuit 112 with a master key Mk and then ciphered by a ciphering circuit 104 with the key Mk, so that the key Sk' generated by the circuit 111 is obtained. Then, a 1st session key ciphered by the key Mk recorded on a DVD 101 is ciphered by the key Sk' and is sent to the circuit 112, where this key is decoded by the key Mk to obtain the 1st session key Mk. Then, a data ciphered by a key Sk recorded on the DVD 101 is read out, and is processed by a demodulation/ error correction circuit 118, and afterward, the received data is decoded by the circuit 112 with the key Sk to obtain a plain styled data. Thus, the decoded data does not flow in a CPU.BUS 110, and for example, even when this data is stored in a storage medium, the data cannot be reproduced to be used. Consequently, an illegal act of making unauthorized copies is prevented to protect the copyright from piracy.



LEGAL STATUS
[Date of request for examination] 16.12.1998

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－106148

(43)公開日　平成10年(1998)４月24日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ
Ｇ０９Ｃ　1/00	６３０	Ｇ０９Ｃ　1/00	６３０Ａ
			６３０Ｅ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ

審査請求　未請求　請求項の数16　ＯＬ　（全 32 頁）　最終頁に続く

(21)出願番号　特願平9－136709

(22)出願日　平成９年(1997)５月27日

(31)優先権主張番号　特願平8－170399

(32)優先日　平８(1996)６月28日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　加藤　岳久
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　遠藤　直樹
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　海野　裕明
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

(74)代理人　弁理士　鈴江　武彦　（外６名）

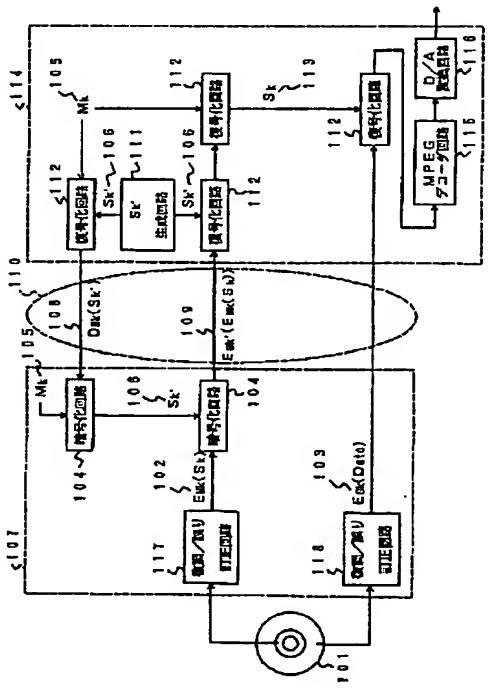
最終頁に続く

(54)【発明の名称】　暗号化方法、復号方法、記録再生装置、復号装置、復号化ユニット装置、記録媒体、記録媒体の製造方法および鍵の管理方法

(57)【要約】

【課題】　ディジタル記録された記録媒体からの不正なコピーを防止するための復号方法を提供すること。

【解決手段】　本発明に係る復号方法は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも入力し、前記第２の鍵の少なくとも一つを用いて前記第１の鍵を復号して得て、得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得ることを特徴とする。また、記録媒体に、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも記録する。



1

【特許請求の範囲】

【請求項１】第１の鍵でデータを暗号化し、前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化することを特徴とする暗号化方法。

【請求項２】データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも記録したことを特徴とする記録媒体。

【請求項３】データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを同一の記録媒体内に少なくとも記録することを特徴とする記録媒体の製造方法。

【請求項４】データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも入力し、

前記第２の鍵の少なくとも一つを用いて前記第１の鍵を復号して得て、

得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得ることを特徴とする復号方法。

【請求項５】データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも入力する入力手段と、

前記第２の鍵の少なくとも一つを記憶する記憶手段と、

この記憶手段内の前記第２の鍵の少なくとも一つを用いて前記入力手段から入力された情報に基づいて前記第１の鍵を復号して得て、得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得る復号手段とを備えたことを特徴とする復号装置。

【請求項６】データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、

前記第２の鍵の少なくとも一つを記憶する記憶手段と、

この記憶手段内の前記第２の鍵の少なくとも一つを用いて前記読み出し手段から読み出された情報に基づいて前記第１の鍵を復号して得て、得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得る復号手段とを備えたことを特徴とする記録再生装置。

【請求項７】第１の管理者に予め定められた複数の第２の鍵を少なくとも保管させ、第２の管理者にデータを第１の鍵で暗号化した情報と前記第１の鍵を前記予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも管理させ、第３の管理者に前記第２の鍵の少なくとも１つを管理させることを特徴とする鍵の管理方法。

【請求項８】データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の

2

鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、

前記第２の鍵の少なくとも一つを記憶する記憶手段と、

前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、

この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記データを復号して得る第２の復号手段とを備えたことを特徴とする復号装置。

【請求項９】記録媒体から少なくとも読み出された、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続された第１のユニットから計算機のＣＰＵバスを介して第２のユニットに伝え、前記第２のユニットにおいて少なくとも前記データの復号を行う復号装置であって、

前記第１のユニットは、前記計算機のＣＰＵバスを介して前記第２のユニットへ、前記第１、第２および第３の情報を伝えるとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に伝えるための手段を備え、

前記第２のユニットは、前記計算機のＣＰＵバスを介して前記第１のユニットから、前記第１、第２および第３の情報を受け取るとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に受け取るための手段と、

前記第２の鍵の少なくとも一つを記憶する記憶手段と、

前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、

この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記データを復号して得る第２の復号手段とを備えたことを特徴とする復号装置。

【請求項１０】第３の鍵を第１の鍵で暗号化して得られ

た第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、

前記第２の鍵の少なくとも一つを記憶する記憶手段と、

前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、

この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得る第２の復号手段と、

この第２の復号手段に得られた前記第３の鍵を用いて前記データを復号して得る第３の復号手段とを備えたことを特徴とする復号装置。

【請求項１１】前記第３の情報は、前記第１の鍵を前記第１の鍵自身で暗号化して得られた情報であり、

前記第１の復号手段は、前記記憶手段に記憶されている前記第２の鍵の一つを用いて前記第２の情報のうちの一つを復号して得られた鍵と、この鍵を用いて前記前記第３の情報を復号して得られた鍵とが一致した場合に、この鍵が正しい第１の鍵であると判定するものであることを特徴とする請求項８ないし１０のいずれか１項に記載の復号装置。

【請求項１２】前記データは、鍵情報、文書、音声、画像およびプログラムのうちの少なくとも１つを含むものであることを特徴とする請求項８ないし１１のいずれか１項に記載の復号装置。

【請求項１３】データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出し、

前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、

正しいものとして得られた前記第１の鍵を用いて前記データを復号して得ることを特徴とする復号方法。

【請求項１４】記録媒体から少なくとも読み出された、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続された第１のユニットから計算機のＣＰＵバスを介して第２のユニットに伝えるとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に伝え、

前記第２のユニットにて、前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第１の鍵を用いて前記データを復号して得ることを特徴とする復号方法。

【請求項１５】第３の鍵を第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し、

前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、

正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得て、

得られた前記第３の鍵を用いて前記データを復号して得ることを特徴とする復号方法。

【請求項１６】記録媒体から少なくとも読み出された、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とが、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続されたバス転送用ユニットから計算機のＣＰＵバスを介して伝えられ、これら情報をもとに前記データを復号する復号化ユニット装置であって、

前記バス転送用ユニットとの間で前記計算機のＣＰＵバスを介して、少なくとも前記第２および第３の情報を外部から取得されることなく安全に受け渡しするための手

5

段と、
前記第２の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、
この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記データを復号して得る第２の復号手段とを備えたことを特徴とする復号化ユニット装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタル記録されたデータに対して記録媒体からのコピーを防止するための暗号化方法、復号方法、記録再生装置、復号装置、復号化ユニット装置、記録媒体、記録媒体の製造方法および鍵の管理方法に関する。

【０００２】

【従来の技術】従来、ディジタル化された情報（例えば、文書、音声、画像、プログラムなど）を記録する媒体として、音声や画像の記録媒体ではコンパクトディスクやレーザディスクがある。また、コンピュータなどのプログラムやデータの記録媒体には、フロッピーディスクやハードディスクがある。また、これら記録媒体に加えて、大容量記録媒体であるＤＶＤ（ディジタルビデオディスク）が開発されている。

【０００３】上記のような種々のディジタル記録媒体において、記録するときにそのままのディジタルデータ（圧縮や符号化等されデコード可能なものも含む）を記録しているため、記録されたデータを他の媒体にコピーすることは、例えば音質や画質の損失なしに、かつ容易にコピーすることが可能であり、複製を大量に作り出すことができ、著作権の侵害など問題があった。

【０００４】

【発明が解決しようとする課題】上述したように、ディジタル記録媒体からコピーする場合、音質や画質の劣化がなく、マスターの音質や画質を保ったままコピーすることができる。このため、海賊版と呼ばれる不正なコピーにより、著作料を払うことなくメディアを販売する不法な行為が可能となるなどの問題があった。

【０００５】本発明は、上記事情を考慮してなされたもので、ディジタル記録された記録媒体からの不正なコピーを防止するための暗号化方法、復号方法、記録再生装置、復号装置、復号化ユニット装置、記録媒体、記録媒体の製造方法および鍵の管理方法を提供することを目的とする。

6

【０００６】

【課題を解決するための手段】本発明（請求項１）に係る暗号化方法は、第１の鍵でデータを暗号化し、前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化することを特徴とする。

【０００７】本発明（請求項２）に係る記録媒体は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも記録したことを特徴とする。

【０００８】本発明（請求項３）に係る記録媒体の製造方法は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを同一の記録媒体内に少なくとも記録することを特徴とする。

【０００９】本発明（請求項４）に係る復号方法は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも入力し、前記第２の鍵の少なくとも一つを用いて前記第１の鍵を復号して得て、得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得ることを特徴とする。

【００１０】本発明（請求項５）に係る復号装置は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも入力する入力手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、この記憶手段内の前記第２の鍵の少なくとも一つを用いて前記入力手段から入力された情報に基づいて前記第１の鍵を復号して得て、得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得る復号手段とを備えたことを特徴とする。

【００１１】本発明（請求項６）に係る記録再生装置は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、この記憶手段内の前記第２の鍵の少なくとも一つを用いて前記読み出し手段から読み出された情報に基づいて前記第１の鍵を復号して得て、得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得る復号手段とを備えたことを特徴とする。

【００１２】本発明（請求項７）に係る鍵の管理方法は、第１の管理者に予め定められた複数の第２の鍵を少なくとも保管させ、第２の管理者にデータを第１の鍵で暗号化した情報と前記第１の鍵を前記予め定められた複

数の第２の鍵でそれぞれ暗号化した情報とを少なくとも管理させ、第３の管理者に前記第２の鍵の少なくとも１つを管理させることを特徴とする。

【００１３】本発明によれば、複数の第２の鍵のうちの少なくとも１つを持つ正当なもののみが、第１の鍵を得ることができ、従って第１の鍵で暗号化されたデータのプレインデータを得ることができる。

【００１４】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【００１５】本発明（請求項８）に係る復号装置は、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記データを復号して得る第２の復号手段とを備えたことを特徴とする。

【００１６】本発明（請求項９）は、記録媒体から少なくとも読み出された、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続された第１のユニットから計算機のＣＰＵバスを介して第２のユニットに伝え、前記第２のユニットにおいて少なくとも前記データの復号を行う復号装置であって、前記第１のユニットは、前記計算機のＣＰＵバスを介して前記第２のユニットへ、前記第１、第２および第３の情報を伝えるとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に伝えるための手段を備え、前記第２のユニットは、前記計算機のＣＰＵバスを介して前記第１のユニットから、前記第１、第２および第３の情報を受け取るとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に受け取るための手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記データを復号して得る第２の復号手段とを備えたことを特徴とする。

【００１７】本発明（請求項１０）に係る復号装置は、第３の鍵を第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得る第２の復号手段と、この第２の復号手段に得られた前記第３の鍵を用いて前記データを復号して得る第３の復号手段とを備えたことを特徴とする。

【００１８】本発明は、記録媒体から少なくとも読み出された、第３の鍵を第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続された第１のユニットから計算機のＣＰＵバスを介して第２のユニットに伝え、前記第２のユニットにおいて少なくとも前記データの復号を行う復号装置であって、前記第１のユニットは、前記計算機のＣＰＵバスを介して前記第２のユニットへ、前記第１、第２、第３および第４の情報を伝えるとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に伝えるための手段を備え、前記第２のユニットは、前記計算機のＣＰＵバスを介して前記第１のユニットから、前記第１、第２、第３および第４の情報を受け取るとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に受け取るための手段と、前記第２の鍵の少なくと

も一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得る第２の復号手段と、この第２の復号手段に得られた前記第３の鍵を用いて前記データを復号して得る第３の復号手段とを備えたことを特徴とする。

【００１９】好ましくは、前記第３の情報は、前記第１の鍵を前記第１の鍵自身で暗号化して得られた情報であり、前記第１の復号手段は、前記記憶手段に記憶されている前記第２の鍵の一つを用いて前記第２の情報のうちの一つを復号して得られた鍵と、この鍵を用いて前記前記第３の情報を復号して得られた鍵とが一致した場合に、この鍵が正しい第１の鍵であると判定するものである。

【００２０】好ましくは、前記データは、鍵情報、文書、音声、画像およびプログラムのうちの少なくとも１つを含むものである。

【００２１】本発明（請求項１３）に係る復号方法は、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出し、前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第１の鍵を用いて前記データを復号して得ることを特徴とする。

【００２２】本発明（請求項１４）に係る復号方法は、記録媒体から少なくとも読み出された、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続された第１のユニットから計算機のＣＰＵバスを介して第２のユニットに伝えるとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全

に伝え、前記第２のユニットにて、前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第１の鍵を用いて前記データを復号して得ることを特徴とする。

【００２３】本発明（請求項１５）に係る復号方法は、第３の鍵を第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し、前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得て、得られた前記第３の鍵を用いて前記データを復号して得ることを特徴とする。

【００２４】本発明に係る復号方法は、記録媒体から少なくとも読み出された、第３の鍵を第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続された第１のユニットから計算機のＣＰＵバスを介して第２のユニットに伝えるとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に伝え、前記第２のユニットにて、前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得て、得られた前記第３の鍵を用いて前記データを復号して得ることを特徴とする。

【００２５】本発明（請求項１６）は、記録媒体から少

なくとも読み出された、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とが、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続されたバス転送用ユニットから計算機のＣＰＵバスを介して伝えられ、これら情報をもとに前記データを復号する復号化ユニット装置であって、前記バス転送用ユニットとの間で前記計算機のＣＰＵバスを介して、少なくとも前記第２および第３の情報を外部から取得されることなく安全に受け渡しするための手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記データを復号して得る第２の復号手段とを備えたことを特徴とする。

【００２６】本発明は、記録媒体から少なくとも読み出された、第３の鍵を第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とが、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続されたバス転送用ユニットから計算機のＣＰＵバスを介して伝えられ、これら情報をもとに前記データを復号する復号化ユニット装置であって、前記バス転送用ユニットとの間で前記計算機のＣＰＵバスを介して、少なくとも前記第２および第３の情報を外部から取得されることなく安全に受け渡しするための手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得る第２の復号手段と、この第２の復号手段に得られた前記第３の鍵を用いて前記データを復号して得る第３の復号手段とを備えたことを特徴とする。

【００２７】本発明に係る記録媒体は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報と鍵判定に用いる情報（例えば、前記第１の鍵を前記第１の鍵自身で暗号化した情報）とを少なくとも記録したことを特徴とする。

【００２８】本発明に係る記録媒体は、第３の鍵を第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とデータを前記第３の鍵で暗号化した情報とを少なくとも記録したことを特徴とする。

【００２９】本発明に係る記録媒体は、第３の鍵を第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報と鍵判定に用いる情報（例えば、前記第１の鍵を前記第１の鍵自身で暗号化した情報）とデータを前記第３の鍵で暗号化した情報とを少なくとも記録したことを特徴とする。

【００３０】本発明によれば、複数の第２の鍵のうちの少なくとも１つを持つ正当なもののみが、第１の鍵を得ることができ、従って第１の鍵で暗号化されたデータのプレインデータを得ることができる。この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【００３１】また、本発明によれば、暗号化ユニットと復号化ユニットとを接続する信号線に流れるデータを保存したとしても、該データは暗号化されたものであり、また、該データを暗号化するために必要な情報は、乱数をもとにして生成されるものであって、後に再現できないために、たとえ、復号ユニット内の第２の鍵（マスターキー）が破られたとしても、保存したデータを再生または利用することはできない。この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。また、本発明によれば、暗号化ユニットおよび復号化ユニットは、ディジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、暗号化ユニットおよび復号化ユニットを交換するだけで良い。

【００３２】また、本発明１は、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められたマスターキーで暗号化された第１のセッションキーとを記録した記録媒体から該デジタル・データの平文を得るための復号方法であって、復号化ユニットにて、所定の乱数をもとにして第２のセッションキーを生成し、生成された第２のセッションキーを前記マスターキーで復号し、復号化ユニットから暗号化ユニットへ、前記マスターキーで復号された第２のセッションキーを伝送し、暗号化ユニットにて、伝送された前記マスターキーで復号された第２のセッションキーを、前記マスターキーで暗号化して、前記第２のセッションキーを取り出

し、暗号化ユニットにて、取り出された前記第２のセッションキーを用いて、前記記録媒体から読み出された前記マスターキーで暗号化された第１のセッションキーを暗号化し、暗号化ユニットから復号化ユニットへ、第２のセッションキーを用いて暗号化された、前記マスターキーで暗号化された第１のセッションキーを伝送し、復号化ユニットにて、伝送された前記第２のセッションキーを用いて暗号化された、前記マスターキーで暗号化された第１のセッションキーを、前記第２のセッションキーを用いて復号し、前記マスターキーで暗号化された第１のセッションキーを取り出し、さらに取り出された前記マスターキーで暗号化された第１のセッションキーを、前記マスターキーで復号して、前記第１のセッションキーを取り出し、取り出された前記第１のセッションキーを用いて、前記記録媒体から読み出された前記第１のセッションキーで暗号化されたデジタル・データを復号して、前記デジタル・データの平文を得ることを特徴とする。

【００３３】本発明２は、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーのうちの所定のマスターキーで暗号化された第１のセッションキーと、第１のセッションキー自身で暗号化された第１のセッションキーとを記録した記録媒体から該デジタル・データの平文を得るための復号方法であって、復号化ユニットにて、所定の乱数をもとにして第２のセッションキーを生成し、生成された第２のセッションキーを予め定められたマスターキーで復号し、復号化ユニットから暗号化ユニットへ、前記予め定められたマスターキーで復号された第２のセッションキーを伝送し、暗号化ユニットにて、伝送された前記予め定められたマスターキーで復号された第２のセッションキーを、前記予め定められたマスターキーで暗号化して、前記第２のセッションキーを取り出し、暗号化ユニットにて、取り出された前記第２のセッションキーを用いて、前記記録媒体から読み出された前記所定のマスターキーで暗号化された第１のセッションキーを暗号化するとともに、取り出された前記第２のセッションキーを用いて、前記記録媒体から読み出された前記第１のセッションキー自身で暗号化された第１のセッションキーを暗号化し、暗号化ユニットから復号化ユニットへ、第２のセッションキーを用いて暗号化された、前記所定のマスターキーで暗号化された第１のセッションキーを伝送するとともに、第２のセッションキーを用いて暗号化された、前記第１のセッションキー自身で暗号化された第１のセッションキーを伝送し、復号化ユニットにて、伝送された前記第２のセッションキーを用いて暗号化された、前記所定のマスターキーで暗号化された第１のセッションキーを、前記第２のセッションキーを用いて復号し、前記所定のマスターキーで暗号化された第１のセッションキーを取り出すとともに、伝送された前記第２のセッションキーを用いて暗号化された、前記第１のセッションキー自身で暗号化された第１のセッションキーを、前記第２のセッションキーを用いて復号し、前記第１のセッションキー自身で暗号化された第１のセッションキーを取り出し、復号化ユニットにて、取り出された前記所定のマスターキーで暗号化された第１のセッションキーを、予め定められた複数のマスターキーのうちのいずれかで復号した第１のセッションキー候補と、取り出された前記第１のセッションキー自身で暗号化された第１のセッションキーを、該第１のセッションキー候補で復号したものとが一致した場合に、該第１のセッションキー候補を前記所定の第１のセッションキーとし、得られた前記第１のセッションキーを用いて、前記記録媒体から読み出された前記第１のセッションキーで暗号化されたデジタル・データを復号して、前記デジタル・データの平文を得ることを特徴とする。

【００３４】本発明３は、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーで夫々暗号化された第１のセッションキーと、第１のセッションキー自身で暗号化された第１のセッションキーとを記録した記録媒体から該デジタル・データの平文を得るための復号方法であって、復号化ユニットにて、所定の乱数をもとにして第２のセッションキーを生成し、生成された第２のセッションキーを予め定められたマスターキーで復号し、復号化ユニットから暗号化ユニットへ、予め定められたマスターキーで復号された第２のセッションキーを伝送し、暗号化ユニットにて、伝送された予め定められたマスターキーで復号された第２のセッションキーを、予め定められたマスターキーで暗号化して、前記第２のセッションキーを取り出し、暗号化ユニットにて、取り出された前記第２のセッションキーを用いて、前記記録媒体から読み出された前記マスターキーで暗号化された第１のセッションキーを暗号化するとともに、取り出された前記第２のセッションキーを用いて、前記記録媒体から読み出された前記第１のセッションキー自身で暗号化された第１のセッションキーを暗号化し、暗号化ユニットから復号化ユニットへ、第２のセッションキーを用いて暗号化された、前記マスターキーで暗号化された第１のセッションキーを伝送するとともに、第２のセッションキーを用いて暗号化された、前記第１のセッションキー自身で暗号化された第１のセッションキーを伝送し、復号化ユニットにて、伝送された前記第２のセッションキーを用いて暗号化された、前記マスターキーで暗号化された第１のセッションキーを、前記第２のセッションキーを用いて復号し、前記マスターキーで暗号化された第１のセッションキーを取り出すとともに、伝送された前記第２のセッションキーを用いて暗号化された、前記第１のセッションキー自身で暗号化された第１のセッションキーを、前記第２のセッションキーを用いて復号し、前記第１のセッ

15

ションキー自身で暗号化された第１のセッションキーを取り出し、復号化ユニットにて、取り出された前記マスターキーで暗号化された第１のセッションキーを、予め定められたマスターキーで復号した第１のセッションキー候補と、取り出された前記第１のセッションキー自身で暗号化された第１のセッションキーを、該第１のセッションキー候補で復号したものとが一致した場合に、該第１のセッションキー候補を前記所定の第１のセッションキーとし、得られた前記第１のセッションキーを用いて、前記記録媒体から読み出された前記第１のセッションキーで暗号化されたデジタル・データを復号して、前記デジタル・データの平文を得ることを特徴とする。

【００３５】本発明４は、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーで夫々暗号化された第１のセッションキーと、第１のセッションキー自身で暗号化された第１のセッションキーとを記録した記録媒体から該デジタル・データの復号に用いる第１のセッションキーを得るための復号方法であって、前記マスターキーで暗号化された第１のセッションキーを、前記複数のマスターキーのうちの予め定められたものをで復号して第１のセッションキー候補を生成し、生成された前記第１のセッションキー候補を用いて、前記第１のセッションキー自身で暗号化された第１のセッションキーを復号し、前記第１のセッションキー候補と、該第１のセッションキー候補を用いて復号された、前記第１のセッションキー自身で暗号化された第１のセッションキーとを比較し、前記比較にて一致した場合に、前記第１のセッションキー候補を前記所定の第１のセッションキーとして決定することを特徴とする。

【００３６】本発明５は、上記発明１ないし３のいずれか１つの発明において、前記暗号化ユニットおよび前記復号化ユニットは、それぞれ、独立して形成された集積回路素子であることを特徴とする。

【００３７】本発明６は、上記発明１ないし３のいずれか１つの発明において、前記暗号化ユニットと前記復号化ユニットとの間で行われる伝送は、ＣＰＵ　ＢＵＳを用いて行われることを特徴とする。

【００３８】本発明７は、上記発明１ないし３のいずれか１つの発明において、前記所定の乱数は、少なくとも前記記録媒体を再生する度に変化するものであることを特徴とする。

【００３９】本発明８は、上記発明１ないし３のいずれか１つの発明において、前記所定の乱数は、所定のタイミングで得られる時間情報をもとにして生成されることを特徴とする。

【００４０】所定のタイミングは、例えば、前記記録媒体がその駆動装置に装着されたタイミングである。

【００４１】本発明９は、上記発明１ないし４のいずれか１つの発明において、前記データは、鍵情報、文書、

16

音声、画像およびプログラムのうちの少なくとも１つを含むものであることを特徴とする。

【００４２】本発明１０は、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められたマスターキーで暗号化された第１のセッションキーとを記録した記録媒体から該デジタル・データの平文を得るための復号装置であって、復号化ユニット内に設けられ、所定の条件に応じて異なる第２のセッションキーを生成する第２のセッションキー生成手段と、生成された前記第２のセッションキーを前記復号化ユニット内で前記マスターキーにて復号し、このデータを暗号化ユニット内へ伝送し、前記暗号化ユニット内で前記マスターキーで暗号化することにより前記第２のセッションキーを取り出す手段と、この手段により取り出された第２のセッションキーを用いて、前記記録媒体から読み出された前記マスターキーで暗号化された前記第１のセッションキーを暗号化し前記復号化ユニットへ伝送する手段と、この手段により復号化ユニット内へ伝送された暗号化された第１のセッションキーを前記復号化ユニット内で生成された第２のセッションキーを用いて復号した後にさらに前記マスターキーを用いて復号して前記第１のセッションキーを得る手段と、この手段により得られた前記第１のセッションキーを用いて、前記記録媒体から読み出された前記第１のセッションキーで暗号化されたデジタル・データを復号して、前記デジタル・データの平文を得る手段とを備えたことを特徴とする。

【００４３】本発明１１は、上記発明１０において、前記第２のセッションキー生成手段は、前記記録媒体の復号操作を行うごとに、あるいは時間情報に応じて異なる第２のセッションキーを生成することを特徴とする。

【００４４】本発明１２に係る記録媒体は、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーで夫々暗号化された第１のセッションキーと、第１のセッションキー自身で暗号化された第１のセッションキーとを記録したことを特徴とする。

【００４５】記録媒体は、例えば、ＤＶＤ、ＣＤ－ＲＯＭ、フロッピーディスク、ハードディスクなど、種々のものに適用可能である。

【００４６】なお、以上の装置に係る各発明は、それぞれ、方法に係る発明や記憶媒体に係る発明としても成立し、以上の方法に係る各発明は、それぞれ、装置に係る発明や記憶媒体に係る発明としても成立する。

【００４７】本発明によれば、暗号化ユニットと復号化ユニットとを接続する信号線に流れるデータを保存したとしても、該データは暗号化されたものであり、また、該データを暗号化するために必要な情報は、乱数をもとにして生成されるものであって、後に再現できないために、たとえ、復号ユニット内のマスターキーが破られたとしても、保存したデータを再生または利用することは

できない。

【００４８】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【００４９】また、本発明によれば、暗号化ユニットおよび復号化ユニットは、ディジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、暗号化ユニットおよび復号化ユニットを交換するだけで良い。

【００５０】また、本発明によれば、記録媒体に、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーのうちの所定のマスターキーで暗号化された第１のセッションキーと、第１のセッションキー自身で暗号化された第１のセッションキーとを記録しておくことにより、前記所定のマスターキーが複数のマスターキーのうちのいずれであっても、複数のマスターキーを持つ復号化ユニットにより、第１のセッションキーを取り出し、この第１のセッションキーにより、データを復号することができる。

【００５１】また、本発明によれば、記録媒体に、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーで夫々暗号化された第１のセッションキーと、第１のセッションキー自身で暗号化された第１のセッションキーとを記録しておくことにより、前記複数のマスターキーのうちのいずれかを少なくとも１つでも持つ復号化ユニットにより、第１のセッションキーを取り出し、この第１のセッションキーにより、データを復号することができる。

【００５２】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【００５３】本実施形態では、あるデータａを鍵Ｋを用いて暗号化する操作をE_K（ａ）と表現し、あるデータａを鍵Ｋを用いて復号化する操作をD_K（ａ）と表現する。この表現を用いることにより、例えば、あるデータａを鍵Ｋを用いて暗号化し復号する操作は、D_K（E_K（ａ））で表される。

【００５４】また、本実施形態では、あるデータをまず復号化し、その後、復号化されたデータを暗号化してもとのデータに戻すことがある。これは、暗号の性質上、データの復号化に暗号化と同等の作用があることに基づいている。つまり、復号化したデータをもとに戻すためには復号化に用いた鍵がわからなければならず、鍵が判れば復号化したデータを暗号化することにより最初に復号化したデータが得られる。この操作は、暗号鍵をｘとしデータをｙとすれば、

E_x（D_x（ｙ））＝ｙ

で表される。

【００５５】本実施形態では、ＤＶＤに記録された、ＭＰＥＧ２というデータ圧縮規格に従って圧縮され暗号化された画像データを、読み出し復号しデコードして再生するシステムを例にとって説明する。

【００５６】（第１の実施形態）以下、第１の実施形態について説明する。

【００５７】図１は、本発明の第１の実施形態に係るシステムの構成を示すブロック図である。また、本実施形態の動作の一例を図２のフローチャートに示す。

【００５８】本実施形態に係るシステムは、パーソナル・コンピュータなどの計算機内に備えられた再生に用いるＣＰＵ（図示せず）のいわゆるＣＰＵ　ＢＵＳに接続されるものであり、暗号化されたデータ（後述するE_{SK}（Ｄａｔａ））がＣＰＵ　ＢＵＳ上を流れる構成を有するものである。なお、図１では、再生に用いるＣＰＵに関する部分のみ示している。

【００５９】図１に示すように、本実施形態に係るシステムは、ＤＶＤ１０１からデータを読み出すＤＶＤ駆動装置（図示せず）、このＤＶＤ駆動装置にＣＰＵ　ＢＵＳを介さずに接続されたまたはＤＶＤ駆動装置に内蔵された暗号化ユニット１０７、復号化ユニット１１４を備えている。

【００６０】暗号化ユニット１０７と復号化ユニット１１４は、ＣＰＵ　ＢＵＳ１１０に接続されている。復号化ユニット１１４からのデータの出力は、ＣＰＵ　ＢＵＳ以外の例えばＩ／Ｏポート等を通じて行われる。つまり、本実施形態では、データの入出力はＣＰＵ　ＢＵＳを介さずに行われるが、暗号化ユニット１０７と復号化ユニット１１４との間でのデータ転送には、ＣＰＵ　ＢＵＳが用いられる。

【００６１】暗号化ユニット１０７は、復調／誤り訂正回路１１７、復調／誤り訂正回路１１８、暗号化回路１０４を備えている。図１中で、暗号化ユニット１０７内には、２つの暗号化回路１０４を示しているが、実際には１つの暗号化回路であるものとする。暗号化ユニット１０７は、独立した１つのＩＣチップとして形成されるものとする。なお、復調／誤り訂正回路１１７および復調／誤り訂正回路１１８は、暗号化ユニット１０７内には備えず、その前段のユニット等の側（ＤＶＤ駆動装置内）に備えられる場合もある。

【００６２】一方、復号化ユニット１１４は、復号化回路１１２、第２のセッションキーS_K´を生成するセッションキー生成回路１１１を備えている。また、本実施形態では、復号化ユニット１１４内にＭＰＥＧのデコーダ回路１１５および復号された画像データをディジタルからアナログに変換する変換回路１１６を備えているものとする。図１中で、復号化ユニット１１４内には、４つの復号化回路１１２を示しているが、実際には１つの復号化回路であるものとする。復号化ユニット１１４は、独立した１つのＩＣチップとして形成されるものとする。

【００６３】また、暗号化ユニット１０７内、および復

19

号化ユニット１１４内には、後述するマスターキーが登録されている（作り込まれている）。マスターキーは、利用者が外部から取得できないように、暗号化ユニットのチップ、復号化ユニットのチップそれぞれにおいて、利用者が意図的に取り出せないようにチップ内部の秘匿された領域に記録されているものとする。

【００６４】なお、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該計算機のＣＰＵで実行することにより実現することができる。この制御部による制御の具体例としては、ＤＶＤからのデータの読み出しに関する指示、データ伝送先の指定、復号化ユニット１１４からのデータ出力に関する指示等である。また、この制御部の起動のトリガーは、例えば、ユーザ・インタフェースを介してユーザにより行われる場合と、あるアプリケーションプログラム中のプロセスからかけられる場合などが考えられる。

【００６５】本実施形態では、第１のセッションキーをS_K、第２のセッションキーをS_K'、マスターキーをM_K、画像データ（すなわち暗号化された一纏まりのデータ）をＤａｔａで表す。これらはいずれも平文である。

【００６６】図１中、１０２は第１のセッションキーS_KをマスターキーM_Kを用いて暗号化して生成された$E_{MK}(S_K)$を、１０３は画像データＤａｔａを第１のセッションキーS_Kを用いて暗号化して生成されたE_{SK}（Ｄａｔａ）を、１０５はマスターキーM_Kを、１０６は第２のセッションキーS_K'を、１０８は第２のセッションキーS_K'をマスターキーM_Kを用いて復号した$D_{MK}(S_K')$を、１０９はマスターキーM_Kを用いて暗号化された第１のセッションキー$E_{MK}(S_K)$を第２のセッションキーS_K'を用いて暗号化した$E_{SK'}(E_{MK}(S_K))$を、１１３は第１のセッションキーS_Kをそれぞれ表す。

【００６７】図３に示すように、ＤＶＤ１０１上で、第１のセッションキーS_KをマスターキーM_Kを用いて暗号化して生成された$E_{MK}(S_K)$は、最内周部分の鍵記録領域（リードインエリア）に、画像データＤａｔａを第１のセッションキーS_Kを用いて暗号化して生成されたE_{SK}（Ｄａｔａ）は、データ記録領域（データエリア）に記録されているものとする。

【００６８】以下、図２のフローチャートを参照しながら、本実施形態の動作について説明する。

【００６９】ステップＳ１で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、マスターキーM_Kを用いて暗号化された第１のセッションキー$E_{MK}(S_K)$を読み出し、暗号ユニット１０７内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【００７０】一方、ステップＳ２で、復号化ユニット１１４では、セッションキー生成回路１１１において、乱数、例えば時計（図示せず）からの時間情報を入力として第２のセッションキーS_K'を生成する。そして、復号化回路１１２において、生成された第２のセッションキーS_K'を、マスターキーM_Kを用いて復号して$D_{MK}(S_K')$を生成し、ＣＰＵ　ＢＵＳ１１０を通じて暗号化ユニット１０７に送る。

20

【００７１】上記の乱数を発生するタイミング（例えば時間情報を入力するタイミング）としては、例えば、ＤＶＤ駆動装置にＤＶＤ１０１が装着されたことを示す信号がアサートされたタイミングを用いることができる。

【００７２】あるいは、セッションキー生成回路１１１は、例えば鍵長分の乱数発生器で構成しても良い。なお、全てのビットが０や１になる可能性のある乱数で鍵を生成する場合は、全てのビットが０や１になることがないようにチェック処理等をする必要がある。

【００７３】ステップＳ３で、暗号ユニット１０７では、暗号化回路１０４において、ＣＰＵ　ＢＵＳ１１０を通じて受け取った$D_{MK}(S_K')$を、マスターキーをM_Kを用いて暗号化する。すなわち、

$E_{MK}(D_{MK}(S_K')) = S_K'$

により、復号化ユニット１１４内のセッションキー生成回路１１１で生成された第２のセッションキーS_K'を得ることができる。

【００７４】ここで、セッションキー生成回路１１１で生成された第２のセッションキーS_K'は、ＣＰＵ　ＢＵＳ１１０上で盗まれたとしても解らないようにしてある。

【００７５】次に、ステップＳ４で、暗号ユニット１０７では、上記のようにして得られた第２のセッションキーS_K'を用いて、ＤＶＤ１０１に記録された暗号化された第１のセッションキー$E_{MK}(S_K)$を暗号化して、$E_{SK'}(E_{MK}(S_K))$を生成し、これをＣＰＵ　ＢＵＳ１１０を通じて復号化ユニット１１４へ送る。

【００７６】次に、ステップＳ５で、復号化ユニット１１４では、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取った$E_{SK'}(E_{MK}(S_K))$を、第２のセッションキーS_K'を用いて復号し、

$D_{SK'}(E_{SK'}(E_{MK}(S_K))) = E_{MK}(S_K)$

を得る。

【００７７】さらに、復号化回路１１２において、得られた$E_{MK}(S_K)$を、マスターキーM_Kを用いて復号し、

$D_{MK}(E_{MK}(S_K)) = S_K$

となり、第１のセッションキーS_Kを得ることができる。

【００７８】以上のようにして第１のセッションキーS_Kを得た後、ステップＳ６で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、第１のセッションキーS_Kを用いて暗号化された画像データE_{SK}（Ｄａｔａ）を読み出し、暗号ユニット１０７内に取り込

21

む。その際、復調／誤り訂正回路１１８により復調、データ中の誤り訂正が行われる。そして、Esk（Ｄａｔａ）を、ＣＰＵ　ＢＵＳ１１０を通じて暗号化ユニット１０７に送る。

【００７９】次に、ステップＳ７で、復号化ユニット１１４では、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったEsk（Ｄａｔａ）を、第１のセッションキーSk を用いて復号し、

Dsk（Esk（Ｄａｔａ））＝Ｄａｔａ

となり、暗号化された画像データを復号して、平文のＤａｔａを得ることができる。

【００８０】そして、例えば復号すべきデータ（すなわちEsk（Ｄａｔａ））の処理が終了し、あるいは処理の中止を要求されるまで、上記のステップＳ６とステップＳ７が繰り返し行われる。

【００８１】以上のようにして得られた画像データＤａｔａは、例えばＭＰＥＧ２というデータ圧縮規格に従って圧縮されている場合にはＭＰＥＧデコーダ回路１１５でデコードされ、そしてＤ／Ａ変換回路１１６でアナログ信号に変換された後、図示しないテレビなどの映像装置に送られ、再生される。

【００８２】なお、上記のステップＳ１と、ステップＳ２およびＳ３とは、どちらを先に実行しても構わない。

【００８３】また、ステップＳ６とステップＳ７の実行については、１つのEsk（Ｄａｔａ）の単位で逐次行う方法、あるいはステップＳ６で所定数のEsk（Ｄａｔａ）を読み込み、一旦バッファなどへ格納し、次にステップＳ７でバッファ内のEsk（Ｄａｔａ）を復号する方法、あるいはステップＳ６とステップＳ７をパイプライン処理的に行う方法などが考えられる。

【００８４】また、復号化回路１１２からＭＰＥＧデコーダ回路１１５に画像データEsk（Ｄａｔａ）を渡す際に、１つのＤａｔａの単位で渡しても良いし、所定数のＤａｔａの単位で渡しても良い。

【００８５】以上のように本実施形態によれば、ディジタル化されたデータを暗号化して記録した媒体を再生する場合（暗号化されたデータを復号する場合）に、計算機のＣＰＵ　ＢＵＳに復号されたデータが流れず、また、ＣＰＵ　ＢＵＳに流れる暗号化されたデータの復号に必要な第１のセッションキーの暗号化に用いた第２のセッションキーSk ´は、例えば時間情報のようにデータ再生の度に変わる情報をもとに生成されるため、図４のようにＣＰＵ　ＢＵＳ１１０を流れるデータを信号線２１０からディジタル記憶媒体２１１に保存したとしても、それを再生または利用することはできない。

【００８６】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【００８７】また、本実施形態では、暗号化および復号化に用いる回路は、図１から解るようにＤＶＤなどのディジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、復号化ユニット１１４（あるいは暗号化ユニット１０７および復号化ユニット１１４）を交換するだけで良い。

22

【００８８】なお、本実施形態では、暗号ユニット１０７は１つの暗号化回路を持つものとしたが、２つの暗号化回路を設けても良い。また、復号化ユニット１１４は１つの復号化回路を持つものとしたが、２、３、または４つの復号化回路として設けても良い。これらの場合、対応する暗号化回路と復号化回路をセットで独立化しあるいは共用するのが好ましい。

【００８９】また、対応する暗号化回路と復号化回路をセットで独立化する場合、独立化した対応する暗号化回路および復号化回路では、他の暗号化回路および復号化回路とは異なる暗号方式を採用しても構わない。

【００９０】（第２の実施形態）次に、第２の実施形態について説明する。

【００９１】本実施形態では、例えば、予め定めた複数のマスターキーを用意し、そのうちの１つまたは複数のマスターキーを、復号化ユニットのメーカ（あるいはＤＶＤの制作・販売会社）などの所定の単位ごとに割り当てるような場合に好適な例について説明する。

【００９２】図５は、本発明の第２の実施形態に係るシステムの構成を示すブロック図である。また、本実施形態の動作の一例を図７および図８のフローチャートに示す。

【００９３】本実施形態に係るシステムは、パーソナル・コンピュータなどの計算機内に備えられた再生に用いるＣＰＵ（図示せず）のいわゆるＣＰＵ　ＢＵＳに接続されるものであり、暗号化されたデータ（Esk（Ｄａｔａ））がＣＰＵ　ＢＵＳ上を流れる構成を有するものである。なお、図５では、再生に用いるＣＰＵに関する部分のみ示している。

【００９４】図５に示すように、本実施形態に係るシステムは、ＤＶＤ１０１からデータの読み出すＤＶＤ駆動装置（図示せず）、このＤＶＤ駆動装置にＣＰＵ　ＢＵＳを介さずに接続されたまたはＤＶＤ駆動装置に内蔵された暗号化ユニット１０７、復号化ユニット１１４ａを備えている。

【００９５】暗号化ユニット１０７と復号化ユニット１１４ａは、ＣＰＵ　ＢＵＳ１１０に接続されている。復号化ユニット１１４ａからのデータの出力は、ＣＰＵ　ＢＵＳ以外の例えばＩ／Ｏポート等を通じて行われる。つまり、本実施形態では、データの入出力はＣＰＵ　ＢＵＳを介さずに行われるが、暗号化ユニット１０７と復号化ユニット１１４ａとの間でのデータ転送には、ＣＰＵ　ＢＵＳが用いられる。

【００９６】暗号化ユニット１０７は、復調／誤り訂正回路１１７、復調／誤り訂正回路１１８、暗号化回路１０４を備えている。図１中で、暗号化ユニット１０７内

には、２つの暗号化回路１０４を示しているが、実際には１つの暗号化回路であるものとする。暗号化ユニット１０７は、独立した１つのＩＣチップとして形成されるものとする。なお、復調／誤り訂正回路１１７および復調／誤り訂正回路１１８は、暗号化ユニット１０７内には備えず、その前段のユニット等の側（ＤＶＤ駆動装置内）に備えられる場合もある。

【００９７】一方、復号化ユニット１１４ａは、復号化回路１１２、第２のセッションキーSK´を生成するセッションキー生成回路１１１、鍵判定回路１２０を備えている。

【００９８】ここで、図６に、鍵判定回路１２０の一構成例を示す。この鍵判定回路１２０は、復号化回路１１２、比較回路１２１、ゲート回路１２２を備えている。また、本実施形態では、復号化ユニット１１４ａ内にＭＰＥＧのデコーダ回路１１５および復号された画像データをディジタルからアナログに変換する変換回路１１６を備えているものとする。

【００９９】図５および図６中で、復号化ユニット１１４ａ内には、鍵判定回路１２０内の２つの復号化回路１１２を含めて、全部で５つの復号化回路１１２を示しているが、実際には１つの復号化回路であるものとする。

【０１００】復号化ユニット１１４ａは、独立した１つのＩＣチップとして形成されるものとする。

【０１０１】また、暗号化ユニット１０７内、および復号化ユニット１１４ａ内には、後述するマスターキーが登録されている（作り込まれている）。マスターキーは、利用者が外部から取得できないように、暗号化ユニットのチップ、復号化ユニットのチップそれぞれにおいて、利用者が意図的に取り出せないようにチップ内部の秘匿された領域に記録されているものとする。

【０１０２】なお、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該計算機のＣＰＵで実行することにより実現することができる。この制御部による制御の具体例としては、ＤＶＤからのデータの読み出しに関する指示、データ伝送先の指定、復号化ユニット１１４ａからのデータ出力に関する指示等である。また、この制御部の起動のトリガーは、例えば、ユーザ・インタフェースを介してユーザにより行われる場合と、あるアプリケーションプログラム中のプロセスからかけられる場合などが考えられる。

【０１０３】本実施形態では、第１のセッションキーをSK、第２のセッションキーをSK´、ｎ種類存在するマスターキーのうちのｔ番目のものをMkt（ここでｔ＝１～ｎ）、画像データ（ただし、暗号化された一纏まりのデータ）をＤａｔａで表す。これらはいずれも平文である。

【０１０４】図１中、１０２－１は第１のセッションキーSK をマスターキーMkiを用いて暗号化して生成されたEMKi （SK ）を、１０２－２は第１のセッションキーSK を第１のセッションキーSK 自身で暗号化して生成されたESK（SK ）を、１０３は画像データＤａｔａを第１のセッションキーSK を用いて暗号化して生成されたESK（Ｄａｔａ）を、１０５はマスターキーMkjを、１０６は第２のセッションキーSK ´を、１０８は第２のセッションキーSK ´をマスターキーMkjを用いて復号したDMkj （SK ´）を、１０９－１はマスターキーMkiを用いて暗号化された第１のセッションキーEMKi （SK ）を第２のセッションキーSK ´を用いて暗号化したESK' （EMKi （SK ））を、１０９－２は第１のセッションキーSK 自身で暗号化された第１のセッションキーESK（SK ）を第２のセッションキーSK ´を用いて暗号化したESK' （ESK（SK ））を、１１３は第１のセッションキーSK をそれぞれ表す。

【０１０５】ここで、ＤＶＤ１０１に記録する第１のセッションキーSK をマスターキーMkiを用いて暗号化して生成されたEMKi （SK ）の種類数と、復号化ユニット１１４ａ内に持つマスターキーMkjの種類数の設定について、例えば次に示すように幾つかの方法が考えられる。

【０１０６】（方法１）ＤＶＤ１０１にはｉを１～ｎのいずれかとする１つのマスターキーEMKi （SK ）を記録し、復号化ユニット１１４ａ内にはｊ＝１～ｎのすべてに対応するｎ個のマスターキーMkjを備える。

【０１０７】（方法２）ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のマスターキーEMKi （SK ）を記録し、復号化ユニット１１４ａ内にはｊを１～ｎのいずれかとする１つのマスターキーMkjを備える。

【０１０８】（方法３）上記の（方法２）を拡張したもので、ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のマスターキーEMKi （SK ）を記録し、復号化ユニット１１４ａ内にはｊを１～ｎのうちのから予め選択されたｍ（２＜ｍ＜ｎ）種類のものとするｍ個のマスターキーMkjを備える。

【０１０９】なお、具体的な数値例としては、例えば、ｎ＝１００あるいはｎ＝４００などであり、ｍ＝２，３，あるいは４、あるいは１０などであるが、これらに限定されるものではない。

【０１１０】（方法４）上記の（方法３）においてＤＶＤと復号化ユニットを逆にした例で、ＤＶＤ１０１にはｉを１～ｎのうちのから予め選択されたｍ（２＜ｍ＜ｎ）種類のものとするｍ個のマスターキーEMKi （SK ）を記録し、復号化ユニット１１４ａ内にはｊ＝１～ｎのすべてに対応するｎ個のマスターキーMkjを備える。

【０１１１】（方法５）ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のマスターキーEMKi （SK ）を記録し、復号化ユニット１１４ａ内にはｊ＝１～ｎのすべてに対応するｎ個のマスターキーMkjを備える。

【０１１２】なお、方法３～方法５は、復号のための手

順は同様になる。

【０１１３】図３に示すように、ＤＶＤ１０１上で、第１のセッションキーSK をマスターキーMkiを用いて暗号化して生成された１個（上記の（方法１）の場合）または複数個（上記の（方法２）～（方法５）の場合）のEMKi （SK ）は、最内周部分の鍵記録領域（リードインエリア）に、画像データＤａｔａを第１のセッションキーSK を用いて暗号化して生成されたESK（Ｄａｔａ）は、データ記録領域（データエリア）に記録されているものとする。

【０１１４】また、復号化ユニット１１４内に、ｎ個（上記の（方法１）、（方法４）、（方法５）の場合）、または１個（上記の（方法２）の場合）、またはｍ個（上記の（方法３）の場合）のマスターキーMkjが登録されているものとする。

【０１１５】なお、暗号化ユニット１０７内には、予め定められた１つのマスターキーが登録されているものとする。

【０１１６】以下では、上記の（方法１）、（方法２）、（方法３～方法５）について順次説明する。

【０１１７】まず、上記の（方法１）の場合について図７および図８のフローチャートを参照しながら本実施形態の動作を説明する。

【０１１８】ステップＳ１１で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、第１のセッションキーSK 自身で暗号化された第１のセッションキーESk（SK ）を読み出し、暗号ユニット１０７内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【０１１９】また、ステップＳ１２で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、マスターキーMkiを用いて暗号化された第１のセッションキーEMki （SK ）（ｉ＝１～ｎのいずれか１つ；ここではｉは未知である）を読み出し、暗号ユニット１０７内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【０１２０】一方、ステップＳ１３で、復号化ユニット１１４ａでは、セッションキー生成回路１１１において、乱数、例えば時計（図示せず）からの時間情報を入力として第２のセッションキーSK ´を生成する。そして、復号化回路１１２において、生成された第２のセッションキーSK ´を、マスターキーMkj（ここでｊは１～ｎのうち予め定められたもの）を用いて復号してDMkj （SK ´）を生成し、ＣＰＵ　ＢＵＳ１１０を通じて暗号化ユニット１０７に送る。

【０１２１】上記の乱数を発生するタイミング（例えば時間情報を入力するタイミング）としては、例えば、ＤＶＤ駆動装置にＤＶＤ１０１が装着されたことを示す信号がアサートされたタイミングを用いることができる。

【０１２２】あるいは、セッションキー生成回路１１１は、例えば鍵長分の乱数発生器で構成しても良い。なお、全てのビットが０や１になる可能性のある乱数で鍵を生成する場合は、全てのビットが０や１になることがないようにチェック処理等をする必要がある。

【０１２３】ステップＳ１４で、暗号ユニット１０７では、暗号化回路１０４において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったDMkj （SK ´）を、マスターキーをマスターキーMkj（ここでｊは１～ｎのうち予め定められたもの）を用いて暗号化する。すなわち、

EMkj （DMkj （SK ´））＝SK ´

により、復号化ユニット１１４ａ内のセッションキー生成回路１１１で生成された第２のセッションキーSK ´を得ることができる。

【０１２４】ここで、セッションキー生成回路１１１で生成された第２のセッションキーSK ´は、ＣＰＵ　ＢＵＳ１１０上で盗まれたとしても解らないようにしてある。

【０１２５】次に、ステップＳ１５で、暗号ユニット１０７では、上記のようにして得られた第２のセッションキーSK ´を用いて、ＤＶＤ１０１に記録された暗号化された第１のセッションキーESk（SK ）を暗号化して、ESK' （ESk（SK ））を生成し、これをＣＰＵ　ＢＵＳ１１０を通じて復号化ユニット１１４ａへ送る。

【０１２６】同様に、ステップＳ１６で、暗号ユニット１０７では、上記のようにして得られた第２のセッションキーSK ´を用いて、ＤＶＤ１０１に記録された暗号化された第１のセッションキーEMki （SK ）を暗号化して、ESK' （EMki （SK））を生成し、これをＣＰＵ　ＢＵＳ１１０を通じて復号化ユニット１１４ａへ送る。

【０１２７】次に、ステップＳ１７で、復号化ユニット１１４ａでは、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったESK' （ESk（SK ））を、第２のセッションキーSK ´を用いて復号し、

DSK' （ESK' （ESk（SK ））＝ESk（SK ）

を得る。

【０１２８】同様に、ステップＳ１８で、復号化ユニット１１４ａでは、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったESK' （EMki （SK ））を、第２のセッションキーSK ´を用いて復号し、

DSK' （ESK' （EMki （SK ））＝EMki （SK ）

を得る。

【０１２９】ここで、EMki （SK ）を生成する際に用いられたマスターキーMkiは未知であるため、ステップＳ１９において、以下に示すように鍵判定回路１２０を用いて第１のセッションキーSK を求める。

【０１３０】最初に、鍵判定処理の原理について説明する。

【０１３１】まず、EMki （SK ）を、すべてのマスタ

27

ーキーMkj（ｊ＝１～ｎ）で夫々復号すると、
Skij ＝Dmkj （Emki （Sk ））（ｊ＝１～ｎ）
が得られる。ここで、Skij （ｊ＝１～ｎ）のうちのいずれかが第１のセッションキーSk である。

【０１３２】次に、上記のEsk（Sk ）を用いて、生成されたSkij （ｊ＝１～ｎ）のいずれが第１のセッションキーSk であるかを調べる。

【０１３３】そこで、Esk（Sk ）を、すべての第１のセッションキーの候補Skij （ｊ＝１～ｎ）で夫々復号すると、
Sk ''（ｉ，ｊ）＝Dskij（Esk（Sk ））
が得られる。

【０１３４】ここで、Emki （Sk ）を生成する際に用＊

```
for (i=1;  i<n+1; i++) {
        DS1[i]=DMK[i] (EMki (Sk));
        DS2[i]=DSK[i] (Esk (Sk));
        if (DS1[i]==DS2[i])
        {
                SK1=DS2[i];
                break;
        }
        else
                EXIT_MISMATCH;
}
```

なお、上記手順の２行目は、Mkiを用いてE mki （Sk ）を復号し、これをＤＳ１［ｉ］に代入する操作を示す。

【０１３７】上記手順の３行目は、Skiを用いてE sk（Sk ）を復号し、これをＤＳ２［ｉ］に代入する操作を示す。

【０１３８】上記手順の４行目は、ＤＳ１［ｉ］とＤＳ２［ｉ］が一致するかどうを判断する操作を示す。

【０１３９】上記手順の９行目は、ＤＳ１［ｉ］とＤＳ２［ｉ］が不一致の場合の操作を示す。

【０１４０】さて、例えば図６の鍵判定回路１２０では、復号化回路１１２により、まず、ｊ＝１として、E mki （Sk ）を、マスターキーMkjで復号して、
Skij ＝Dmkj （Emki （Sk ））
を得る。

【０１４１】次に、復号化回路１１２により、Esk（Sk ）をSkij で復号して、
Sk ''＝Dskij（Esk（Sk ））
を得る。

【０１４２】次に、比較回路１２１により、上記のSk ''とＳkij を比較し、一致した場合、ゲート回路１２２を制御して、保持しておいたSkij （図６（ａ））またはSk ''（図６（ｂ））を、第１のセッションキーSk として出力する。

【０１４３】一致しなかった場合、上記のｊを１ずつ増加させながら、同様の動作を、第１のセッションキーSk が得られるまで繰り返す。

28

＊いられたマスターキーMkiと同一のマスターキーMkjを復号化ユニット内で用いた場合に、すなわち、ｉ＝ｊの場合に、Sk ''（ｉ，ｊ）＝Skij ＝Sk となる。

【０１３５】したがって、各Skij （ｊ＝１～ｎ）について、Sk ''（ｉ，ｊ）＝Skij （ｊ＝１～ｎ）が成立するか否かを調べることにより、Sk ''（ｉ，ｊ）＝Skij（ｊ＝１～ｎ）を満足するSkij を、第１のセッションキーSk として得ることができる。なお、このSkij を与えるｊに対応するものが今回使用されたマスターキーである。

【０１３６】この操作を、Ｃ言語の表記を利用してＣ言語的に表現すると、次のようになる。

【０１４４】以上のようにして第１のセッションキーSk を得た後、ステップＳ２０で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、第１のセッションキーSk を用いて暗号化された画像データE sk（Ｄａｔａ）を読み出し、暗号ユニット１０７内に取り込む。その際、復調／誤り訂正回路１１８により復調、データ中の誤り訂正が行われる。そして、Esk（Ｄａｔａ）を、ＣＰＵ　ＢＵＳ１１０を通じて暗号化ユニット１０７に送る。

【０１４５】次に、ステップＳ２１で、復号化ユニット１１４ａでは、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったEsk（Ｄａｔａ）を、第１のセッションキーSk を用いて復号し、
Dsk（Esk（Ｄａｔａ））＝Ｄａｔａ
となり、暗号化された画像データを復号して、平文のＤａｔａを得ることができる。

【０１４６】そして、例えば復号すべきデータ（すなわちEsk（Ｄａｔａ））が終了し、あるいは処理の中止を要求されるまで、上記のステップＳ２０とステップＳ２１が繰り返し行われる。

【０１４７】以上のようにして得られた画像データＤａｔａは、例えばＭＰＥＧ２というデータ圧縮規格に従って圧縮されている場合にはＭＰＥＧデコーダ回路１１５でデコードされ、そしてＤ／Ａ変換回路１１６でアナログ信号に変換された後、図示しないテレビなどの映像装置に送られ、再生される。

【０１４８】なお、上記のステップＳ１１と、ステップ

Ｓ１２と、ステップＳ１３およびＳ１４とは、いずれを先に実行しても構わない。

【０１４９】また、上記のステップＳ１５およびステップＳ１７と、ステップＳ１６およびＳ１８とは、いずれを先に実行しても構わない。

【０１５０】また、ステップＳ２０とステップＳ２１の実行については、１つのEsk（Ｄａｔａ）の単位で逐次行う方法、あるいはステップＳ２０で所定数のEsk（Ｄａｔａ）を読み込み、一旦バッファなどへ格納し、次にステップＳ２１でバッファ内のEsk（Ｄａｔａ）を復号する方法、あるいはステップＳ２０とステップＳ２１をパイプライン処理的に行う方法などが考えられる。

【０１５１】また、復号化回路１１２からＭＰＥＧデコーダ回路１１５に画像データEsk（Ｄａｔａ）を渡す際に、１つのＤａｔａの単位で渡しても良いし、所定数のＤａｔａの単位で渡しても良い。

【０１５２】以上のように本実施形態によれば、第１の実施形態と同様に、ＣＰＵ　ＢＵＳを流れるデータを保存したとしても、それを再生または利用することはできない。

【０１５３】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【０１５４】また、本実施形態によれば、記録媒体に記録した第１のセッションキーを暗号化するのに用いたマスターキーを直接示す情報が不要であり、ＤＶＤなどへの記録の際に予め定められた範囲内で適宜マスターキーを選択して使用することが可能となる。あるいは、ＤＶＤの制作・販売会社などの所定の単位ごとに使用可能なマスターキーを割り当てることができるなどの利点がある。

【０１５５】もちろん、本実施形態でも、暗号化および復号化に用いる回路は、ＤＶＤなどのディジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、復号化ユニット１１４ａ（あるいは暗号化ユニット１０７および復号化ユニット１１４ａ）を交換するだけで良い。

【０１５６】なお、本実施形態では、暗号化ユニット１０７は１つの暗号化回路を持つものとしたが、２つの暗号化回路を設けても良い。また、復号化ユニット１１４ａは１つの復号化回路を持つものとしたが、２、３、４、または５つの復号化回路を設けても良い。これらの場合、対応する暗号化回路と復号化回路をセットで独立化するのが好ましい。

【０１５７】また、対応する暗号化回路と復号化回路をセットで独立化する場合、独立化した対応する暗号化回路と復号化回路では、他の暗号化回路および復号化回路とは異なる暗号方式を採用しても構わない。

【０１５８】次に、前述した（方法２）のように、ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のE

Mki（Sk）を記録し、復号化ユニット１１４ａ内にはｊを１～ｎのいずれかとする１つのMkjを備える場合について図７および図８のフローチャートを参照しながら本実施形態の動作を説明する。

【０１５９】ステップＳ１１で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、第１のセッションキーSk 自身で暗号化された第１のセッションキーEsk（Sk）を読み出し、暗号ユニット１０７内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【０１６０】また、ステップＳ１２で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、マスターキーMkiを用いて暗号化されたｎ個の第１のセッションキーEMki（Sk）（ｉ＝１～ｎ）を読み出し、暗号ユニット１０７内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【０１６１】一方、ステップＳ１３で、復号化ユニット１１４ａでは、セッションキー生成回路１１１において、乱数、例えば時計（図示せず）からの時間情報を入力として第２のセッションキーSk´を生成する。そして、復号化回路１１２において、生成された第２のセッションキーSk´を、マスターキーMkj（ここでｊは１～ｎのうち予め定められたもの）を用いて復号してDMkj（Sk´）を生成し、ＣＰＵ　ＢＵＳ１１０を通じて暗号化ユニット１０７に送る。

【０１６２】上記の乱数を発生するタイミング（例えば時間情報を入力するタイミング）としては、例えば、ＤＶＤ駆動装置にＤＶＤ１０１が装着されたことを示す信号がアサートされたタイミングを用いることができる。

【０１６３】ステップＳ１４で、暗号ユニット１０７では、暗号化回路１０４において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったDMkj（Sk´）を、マスターキーをマスターキーMkj（ここでｊは１～ｎのうち予め定められたもの）を用いて暗号化する。すなわち、

EMkj（DMkj（Sk´））＝Sk´

により、復号化ユニット１１４ａ内のセッションキー生成回路１１１で生成された第２のセッションキーSk´を得ることができる。

【０１６４】ここで、セッションキー生成回路１１１で生成された第２のセッションキーSk´は、ＣＰＵ　ＢＵＳ１１０上で盗まれたとしても解らないようにしてある。

【０１６５】次に、ステップＳ１５で、暗号ユニット１０７では、上記のようにして得られた第２のセッションキーSk´を用いて、ＤＶＤ１０１に記録された暗号化された第１のセッションキーEsk（Sk）を暗号化して、Esk´（Esk（Sk））を生成し、これをＣＰＵ　ＢＵＳ１１０を通じて復号化ユニット１１４ａへ送る。

【０１６６】同様に、ステップＳ１６で、暗号ユニット

31

１０７では、上記のようにして得られた第２のセッションキーSK ´を用いて、ＤＶＤ１０１に記録された暗号化されたｎ個の第１のセッションキーEMKi （SK ）を夫々暗号化して、ESK' （EMKi （SK ））を生成し、これをＣＰＵ　ＢＵＳ１１０を通じて復号化ユニット１１４ａへ送る。

【０１６７】次に、ステップＳ１７で、復号化ユニット１１４ａでは、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったESK' （ESK （SK ））を、第２のセッションキーSK ´を用いて復号し、

DSK' （ESK' （ESK （SK ））＝ESK （SK ）

を得る。

【０１６８】同様に、ステップＳ１８で、復号化ユニット１１４ａでは、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったｎ個のESK' （EMKi （SK ））を、第２のセッションキーSK ´を用いて夫々復号し、

DSK' （ESK' （EMKi （SK ））＝EMKi （SK ）

を得る。

【０１６９】ここで、ＤＶＤ１０１に記録されているｎ個のEMKi （SK ）（ｉ＝１～ｎ）の各々について、それを生成する際に用いられたマスターキーMkiは未知であり、復号化ユニット１１４ａ内に備えられたマスターキーMkjに対応するものがどれなのかは、分からないようになっている。そこで、ステップＳ１９において、以下に示すように鍵判定回路１２０を用いて第１のセッションキーSK を求める。

【０１７０】最初に、鍵判定処理の原理について説明する。

【０１７１】まず、マスターキーMkjで、すべてのEMKi （SK ）（ｉ＝１～ｎ）を夫々復号すると、

SKij ＝DMKj （EMKi （SK ））（ｉ＝１～ｎ）

が得られる。ここで、SKij （ｉ＝１～ｎ）のうちのいずれかが第１のセッションキーSK である。

【０１７２】次に、上記のESK （SK ）を用いて、生成されたSKij （ｉ＝１～ｎ）のいずれが第１のセッションキーSK であるかを調べる。

【０１７３】そこで、ESK （SK ）を、すべての第１のセッションキーの候補SKij （ｉ＝１～ｎ）で夫々復号すると、

SK ''（ｉ，ｊ）＝DSKij （ESK （SK ））

が得られる。

【０１７４】ここで、EMKi （SK ）を生成する際に用いられたマスターキーMkiと同一のマスターキーMkjを復号化ユニット内で用いた場合に、すなわち、ｉ＝ｊの場合に、SK ''（ｉ，ｊ）＝SKij ＝SK となる。

【０１７５】したがって、各SKij （ｉ＝１～ｎ）について、SK ''（ｉ，ｊ）＝SKij （ｊ＝１～ｎ）が成立するか否かを調べることにより、SK ''（ｉ，ｊ）＝SKij （ｊ＝１～ｎ）を満足するSKij を、第１のセッションキーSK として得ることができる。なお、このSKij を与えるｉに対応するものが今回使用されたマスターキーである。

32

【０１７６】さて、例えば図６の鍵判定回路１２０では、復号化回路１１２により、まず、ｉ＝１として、EMKi （SK ）を、マスターキーMkjで復号して、

SKij ＝DMKj （EMKi （SK ））

を得る。

【０１７７】次に、復号化回路１１２により、ESK （SK ）をSKij で復号して、

SK ''＝DSKij （ESK （SK ））

を得る。

【０１７８】次に、比較回路１２１により、上記のSK ''と＝SKij を比較し、一致した場合、ゲート回路１２２を制御して、保持しておいたSKij （図６（ａ））またはSK ''（図６（ｂ））を、第１のセッションキーSK として出力する。

【０１７９】一致しなかった場合、上記のｉを１ずつ増加させながら、同様の動作を、第１のセッションキーSK が得られるまで繰り返す。

【０１８０】以上のようにして第１のセッションキーSK を得た後、前述したようにステップＳ２０～Ｓ２２で、第１のセッションキーSK を使って、暗号化された画像データESK （Ｄａｔａ）から画像データＤａｔａを取り出す。

【０１８１】そして、前述したように、画像データＤａｔａは、ＭＰＥＧデコーダ回路１１５でデコードされ、Ｄ／Ａ変換回路１１６でアナログ信号に変換されるなどして、図示しないテレビなどの映像装置に送られ、再生される。

【０１８２】なお、この方法２の場合においても、上記のステップＳ１１と、ステップＳ１２と、ステップＳ１３およびＳ１４とは、いずれを先に実行しても構わない。

【０１８３】また、上記のステップＳ１５およびステップＳ１７と、ステップＳ１６およびＳ１８とは、いずれを先に実行しても構わない。

【０１８４】さらに、ステップＳ１２，Ｓ１６，Ｓ１８、Ｓ１９を、ＤＶＤに記録されたｎ個の（暗号化された）マスターキーを一括してバッチ的に行っても良いが、所定数個のマスターキーごとにバッチ的に行っても良いし、１つのマスターキーごとに逐次行っても良い。

【０１８５】また、３番目の１つのマスターキーごとに逐次行う場合、第２のセッションキーSK ´を、マスターキーごとに生成しても良い。

【０１８６】また、ステップＳ２０とステップＳ２１の実行については、１つのESK （Ｄａｔａ）の単位で逐次行う方法、あるいはステップＳ２０で所定数のESK （Ｄａｔａ）を読み込み、一旦バッファなどへ格納し、次にステップＳ２１でバッファ内のESK （Ｄａｔａ）を復号

33

する方法、あるいはステップＳ２０とステップＳ２１をパイプライン処理的に行う方法などが考えられる。

【０１８７】また、復号化ユニット１１４からＭＰＥＧデコーダ回路１１５に画像データE_{SK}（Ｄａｔａ）を渡す際に、１つのＤａｔａの単位で渡しても良いし、所定数のＤａｔａの単位で渡しても良い。

【０１８８】以上のように本実施形態によれば、第１の実施形態と同様に、ＣＰＵ　ＢＵＳを流れるデータを保存したとしても、それを再生または利用することはできない。

【０１８９】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【０１９０】また、本実施形態によれば、記録媒体に複数のマスターキーを夫々用いて暗号化した第１のセッションキーと、第１のセッションキー自身で暗号化した第１のセッションキーとを格納するので、復号化ユニット内に作り込むマスターキーを、所定の単位、例えばユニットの製造メーカーごとに割り当てて使用することができるなどの利点がある。

【０１９１】また、本実施形態でも、暗号化および復号化に用いる回路は、図１から解るようにＤＶＤなどのディジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、復号化ユニット１１４ｂ（あるいは暗号化ユニット１０７および復号化ユニット１１４ｂ）を交換するだけで良い。

【０１９２】なお、本実施形態では、暗号ユニット１０７は１つの暗号化回路を持つものとしたが、２つの暗号化回路を設けても良い。また、復号化ユニット１１４ａは１つの復号化回路を持つものとしたが、２、３、４、または５つの復号化回路として設けても良い。これらの場合、対応する暗号化回路と復号化回路をセットで独立化しあるいは共用するのが好ましい。

【０１９３】また、対応する暗号化回路と復号化回路をセットで独立化する場合、独立化した対応する暗号化回路と復号化回路では、他の暗号化回路および復号化回路とは異なる暗号方式を採用しても構わない。

【０１９４】次に、前述した（方法３）のように、ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のE_{MKi}（S_K）を記録し、復号化ユニット１１４ａ内にはｊを１～ｎのうちのｍ（＜ｎ）種類のものとするｍ個のM_{kj}を備える場合について説明する。

【０１９５】この方法３は、基本的な構成・動作・効果は上記の方法２と同様であるので、ここでは、相違点のみを説明する。

【０１９６】上記の方法２では、復号ユニット１１４ａ内に予め定めた１個のマスターキーM_{kj}（ｊ＝１～ｎのいずれか１つ）を備えたが、この方法３では、復号ユニット１１４ａ内に予め定めたｍ（≧２）個のマスターキーM_{kj}を備えておく。そして、ｍ個のマスターキーM_{kj}（ｊ＝１～ｎのいずれかｍ個）について、復号化ユニット１１４ｂ内で前述した鍵判定に使用する順位を決めておく。

34

【０１９７】最初は、ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のE_{MKi}（S_K）を記録しているので、復号化ユニット１１４ｂ内で使用順位が１位のマスターキーを用いれば、第１のセッションキーS_Kを得ることができるので、この場合には、前述の方法２と同様の動作になる。

【０１９８】次に、方法３では、いずれかのマスターキーが破られるなどした場合、そのマスターキーを使用不可とし、以降、ＤＶＤ１０１には使用不可となったマスターキーに対応するE_{MKi}（S_K）を記録しないようにした場合を考える。

【０１９９】ここで、使用不可となったマスターキーが、使用順位が１位のマスターキーでない場合、第１のセッションキーS_Kを得ることができるので、この場合にも、前述の方法２と同様の動作になる。

【０２００】一方、使用順位が１位のマスターキーが使用不可となった場合、ＤＶＤ１０１に該マスターキーに対応するE_{MKi}（S_K）は記録されていないので、この使用順位が１位のマスターキーを使っても、前述のステップＳ１９にて第１のセッションキーS_Kを得ることはできない。このような場合に、復号ユニット１１４ａ内で、使用順位が２位のマスターキーを用いて方法２と同様の動作を行うことにより、このマスターキーが使用不可となっていない場合、第１のセッションキーS_Kを得ることができる。

【０２０１】以下、使用順位がｒ位のマスターキーが使用不可となっても、使用順位がｒ＋１位以降のマスターキーで使用不可となっていないものがある場合、同様にして第１のセッションキーS_Kを得ることができる。

【０２０２】このようにして、復号化ユニット１１４ａ内に予め定めたｍ（≧２）個のマスターキーが全て使用不可となるまで、本復号化ユニット１１４ａを使用することができる。

【０２０３】なお、前述した（方法５）の動作は、上記（方法３）と同様になる。

【０２０４】また、前述した（方法４）は、ＤＶＤ１０１には全てのマスターキーに対応する情報が格納されていないので、復号化ユニット内で選択したマスターキーに対応する情報がＤＶＤ１０１に記録されていない場合には、上記の使用不可の場合と同様に復号できないことになり、次の使用順位のマスターキーを選択して復号を試行することになる。従って、この（方法４）の動作も、上記（方法３）と同様になる。

【０２０５】ところで、本実施形態において、ＣＰＵ　ＢＵＳ１１０上を情報を暗号化して安全に転送するために、第２のセッションキーS_K´を用いた。この第２の

セッションキーSK ´は、復号化ユニット１１４ａ内で生成され、マスターキーを用いた手順により暗号化ユニット１０７に伝えられた。その際、本実施形態では、暗号化ユニット１０７内には、予め定められた１つのマスターキーが登録されているものとした。

【０２０６】その代わりに、暗号化ユニット１０７内にも複数のマスター鍵を登録しておき、鍵判定を用いる前述した（方法１）～（方法５）のような手順を用いて、第２のセッションキーSK ´を復号化ユニット１１４ａから暗号化ユニット１０７に伝えるようにしてもよい。

【０２０７】例えば、復号化ユニット１１４ａ内に登録されているマスターキーと同一のものを暗号化ユニット１０７にも登録する場合、上記の（方法５）になる。

【０２０８】また、復号化ユニット１１４ａ内に登録されているマスターキーの一部の複数のものを暗号化ユニット１０７に登録する場合、上記の（方法３）になる。

【０２０９】なお、暗号化ユニット１０７に１つのマスターキーを登録する場合にも、上記の（方法２）の手順を用いることができる。

【０２１０】ただし、これらの場合、（方法１）～（方法５）の手順において、暗号化と復号とを入れ替えた手順となる。すなわち、復号化ユニット１１４ａから暗号化ユニット１０７にDMKi（SK）とDSK（SK）とを転送することになる。

【０２１１】なお、第２のセッションキーSK ´をＣＰＵ　ＢＵＳ１１０上を介して復号化ユニット１１４ａから暗号化ユニット１０７に安全に伝えるための構成としは、上記のマスターキーを用いる構成の他にも、種々のものが適用可能である。例えば、「日経エレクトロニクス　Ｎｏ．６７６　ｐｐ．１３－１４　１９９６．１１．１８」に開示された技術を応用することもできる。この場合、暗号化ユニット１０７内へのマスターキーの登録は不要である。

【０２１２】（第３の実施形態）次に、第３の実施形態について説明する。

【０２１３】本実施形態は、例えば単体のＤＶＤプレーヤーである。

【０２１４】図９は、本発明の第２の実施形態に係るシステムの構成を示すブロック図である。また、本実施形態の動作の一例を図１０のフローチャートに示す。

【０２１５】本実施形態は、第２の実施形態の構成から、暗号化ユニットと復号ユニットとの間で第２のセッションキーを用いて暗号化鍵を受け渡しする動作に関する部分を削除したものである。

【０２１６】すなわち、図９に示すように、本実施形態に係るシステムは、ＤＶＤ１０１からデータの読み出すＤＶＤ駆動装置（図示せず）、復号化ユニット１１４ｂを備えている。

【０２１７】復号化ユニット１１４ｂは、復号化回路１１２、鍵判定回路１２０、復調／誤り訂正回路１１７、

復調／誤り訂正回路１１８を備えている。また、本実施形態では、復号化ユニット１１４内にＭＰＥＧのデコーダ回路１１５および復号された画像データをディジタルからアナログに変換する変換回路１１６を備えているものとする。

【０２１８】ここで、鍵判定回路１２０は、図６の一構成例に示すように、復号化回路１１２、比較回路１２１、ゲート回路１２２を備えている。

【０２１９】図９および図６中で、復号化ユニット１１４ｂ内には、鍵判定回路１２０内の２つの復号化回路１１２を含めて、全部で３つの復号化回路１１２を示しているが、実際には１つの復号化回路であるものとする。なお、復調／誤り訂正回路１１７および復調／誤り訂正回路１１８は、暗号化ユニット１０７内には備えず、その前段のユニット等の側に備えられる場合もある。

【０２２０】復号化ユニット１１４ｂは、独立した１つのＩＣチップとして形成されるものとする。

【０２２１】また、復号化ユニット１１４ｂ内には、後述するマスターキーが登録されている（作り込まれている）。マスターキーは、利用者が外部から取得できないように、復号化ユニットのチップにおいて、利用者が意図的に取り出せないようにチップ内部の秘匿された領域に記録されているものとする。

【０２２２】本実施形態では、第１のセッションキーをSK 、第２のセッションキーをSK ´、ｎ種類存在するマスターキーのうちのｉ番目のものをMki（ここでｉ＝１～ｎ）、画像データ（ただし、暗号化された一纏まりのデータ）をＤａｔａで表す。これらはいずれも平文である。

【０２２３】図１中、１０２－１は第１のセッションキーSK をマスターキーMkiを用いて暗号化して生成されたEMKi（SK）を、１０２－２は第１のセッションキーSK を第１のセッションキーSK 自身で暗号化して生成されたESK（SK）を、１０３は画像データＤａｔａを第１のセッションキーSK を用いて暗号化して生成されたESK（Ｄａｔａ）を、１０５はマスターキーMkjを、１１３は第１のセッションキーSK をそれぞれ表す。

【０２２４】ここで、前述の第２の実施形態と同様に、ＤＶＤ１０１に記録する第１のセッションキーSK をマスターキーMkiを用いて暗号化して生成されたEMKi（SK）の種類数と、復号化ユニット１１４ｂ内に持つマスターキーMkjの種類数の設定について、例えば次に示すように幾つかの方法が考えられる。

【０２２５】（方法１）ＤＶＤ１０１にはｉを１～ｎのいずれかとする１つのEMKi（SK）を記録し、復号化ユニット１１４ｂ内にはｊ＝１～ｎのすべてに対応するｎ個のMkjを備える。

【０２２６】（方法２）ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のEMKi（SK）を記録し、復号

化ユニット１１４ｂ内にはｊを１～ｎのいずれかとする１つのMkjを備える。

【０２２７】（方法３）ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のEMKi （SK ）を記録し、復号化ユニット１１４ｂ内にはｊを１～ｎのうちのｍ（２＜ｍ＜ｎ）種類のものとするｍ個のMkjを備える。

【０２２８】（方法４）ＤＶＤ１０１にはｉを１～ｎのうちのから予め選択されたｍ（２＜ｍ＜ｎ）種類のものとするｍ個のマスターキーEMKi （SK ）を記録し、復号化ユニット１１４ｂ内にはｊ＝１～ｎのすべてに対応するｎ個のマスターキーMkjを備える。

【０２２９】（方法５）ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のマスターキーEMKi （SK ）を記録し、復号化ユニット１１４ｂ内にはｊ＝１～ｎのすべてに対応するｎ個のマスターキーMkjを備える。

【０２３０】図３に示すように、ＤＶＤ１０１上で、第１のセッションキーSK をマスターキーMkiを用いて暗号化して生成された１個（上記の（方法１）の場合）または複数個（上記の（方法２）～（方法５）の場合）のEMKi （SK ）は、最内周部分の鍵記録領域（リードインエリア）に、画像データＤａｔａを第１のセッションキーSK を用いて暗号化して生成されたESK（Ｄａｔａ）は、データ記録領域（データエリア）に記録されているものとする。

【０２３１】次に、図１０のフローチャートを参照しながら本実施形態の動作について説明する。なお、本実施形態の動作は、第２の実施形態の動作から、暗号化ユニットと復号ユニットとの間で第２のセッションキーを用いて暗号化鍵を受け渡しする動作に関する部分を削除したものである。

【０２３２】すなわち、ステップＳ３１で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、第１のセッションキーSK 自身で暗号化された第１のセッションキーESK（SK ）を読み出し、復号化ユニット１１４ｂ内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【０２３３】また、ステップＳ３２で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、マスターキーMkiを用いて暗号化された第１のセッションキーEMKi （SK ）を読み出し、復号化ユニット１１４ｂ内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【０２３４】次に、ステップＳ３３において、鍵判定回路１２０を用いて第１のセッションキーSK を求める。

【０２３５】以上の第１のセッションキーSK を求める動作は、（方法１）、（方法２）、（方法３～方法５）により相違するが、いずれの場合についても既に第２の実施形態において説明したものと同様であるので、ここでの説明は省略する。

【０２３６】第１のセッションキーSK を得た後は、前

述したようにステップＳ３４～Ｓ３６で、第１のセッションキーSK を使って、暗号化された画像データESK（Ｄａｔａ）から画像データＤａｔａを取り出す。なお、ステップＳ３４～Ｓ３６の動作は、ユニット間でＣＰＵ　ＢＵＳを介した画像データＤａｔａの受け渡しがない以外は、第２の実施形態において既に説明したステップＳ２０～Ｓ２２（すなわち、第１の実施形態において既に説明したステップＳ６～Ｓ８）と同様である。

【０２３７】そして、前述したように、画像データＤａｔａは、ＭＰＥＧデコーダ回路１１５でデコードされ、Ｄ／Ａ変換回路１１６でアナログ信号に変換されるなどして、図示しないテレビなどの映像装置に送られ、再生される。

【０２３８】なお、この方法３の場合においても、上記のステップＳ３１と、ステップＳ３２とは、いずれを先に実行しても構わない。

【０２３９】また、（方法２）および（方法３～５）の場合において、ステップＳ３２、Ｓ３３を、ＤＶＤに記録されたｎ個（方法２，３，５の場合）あるいはｍ個（方法４の場合）の（暗号化された）マスターキーを一括してバッチ的に行っても良いが、所定数個のマスターキーごとにバッチ的に行っても良いし、１つのマスターキーごとに逐次行っても良い。

【０２４０】また、ステップＳ３４とステップＳ３５の実行については、１つのESK（Ｄａｔａ）の単位で逐次行う方法、あるいはステップＳ２０で所定数のESK（Ｄａｔａ）を読み込み、一旦バッファなどへ格納し、次にステップＳ２１でバッファ内のESK（Ｄａｔａ）を復号する方法、あるいはステップＳ２０とステップＳ２１をパイプライン処理的に行う方法などが考えられる。

【０２４１】また、復号化ユニット１１４からＭＰＥＧデコーダ回路１１５に画像データESK（Ｄａｔａ）を渡す際に、１つのＤａｔａの単位で渡しても良いし、所定数のＤａｔａの単位で渡しても良い。

【０２４２】本実施形態によれば、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【０２４３】また、本実施形態によれば、ＤＶＤなどへの記録の際に予め定められた範囲内で適宜マスターキーを選択して使用することが可能となる。あるいは、ＤＶＤプレーヤーのメーカまたはＤＶＤの制作・販売会社などの所定の単位ごとに使用可能なマスターキーを割り当てて使用することができるなどの利点がある。

【０２４４】また、本実施形態では、暗号化および復号化に用いる回路は、図１から解るようにＤＶＤなどのディジタル記録再生機器の再生部分のコアとなる箇所とは別に設計できるため、たとえ暗号が破られたとしても、復号化ユニット１１４ｂを交換するだけで良い。

【０２４５】なお、本実施形態では、復号化ユニット１１４ｂは１つの復号化回路を持つものとしたが、２また

は３つの復号化回路として設けても良い。これらの場合、対応する暗号化回路と復号化回路をセットで独立化しあるいは共用するのが好ましい。

【０２４６】また、対応する暗号化回路と復号化回路をセットで独立化する場合、独立化した対応する暗号化回路および復号化回路では、他の暗号化回路および復号化回路とは異なる暗号方式を採用しても構わない。

【０２４７】以上、第１の実施形態、第２の実施形態（より詳しくは３種類の構成）、第３の実施形態（より詳しくは３種類の構成）について夫々説明してきたが、本発明はこれらに限定されず種々変形して実施することができる。

【０２４８】各実施形態では、情報の記録媒体をＤＶＤとして説明したが、本発明は、ＣＤ－ＲＯＭ等他の記録媒体にも適用可能である。

【０２４９】各実施形態では、復号対象となる情報として画像データを例にとって説明したが、本発明は、音声、テキスト、プログラムなど、他の形態の情報の再生装置等にも適用可能である。

【０２５０】なお、各実施形態では、データＤａｔａを画像データとしたが、データＤａｔａを鍵情報S_{kt}とする構成も考えられる。すなわち、ＤＶＤ等の記録媒体に、E_{SK}（Ｄａｔａ）の代わりに、E_{SK}（S_{kt}）とE_{skt}（Ｄａｔａ）を記録しておき、復号化ユニット１１４，１１４ａ，１１４ｂにおいて各実施形態で示した手順により、まずS_{kt}を得て、このS_{kt}でE_{skt}（Ｄａｔａ）を復号して実際のコンテンツを得るようにすることもできる。また、このような鍵の階層化は、任意の階層に渡って行うことができる。

【０２５１】各実施形態では、復号対象となる情報がＭＰＥＧ２という規格に従って圧縮されている場合を例にとって説明したが、本発明はこれに限定されず、他の規格によってデータ圧縮あるいは符号化等されていても構わない。この場合、ＭＰＥＧデコーダ回路１１５の代わりに、他の対応するデコーダ回路を設ける。また、符号化等されていないものであっても構わない。この場合、ＭＰＥＧデコーダ回路１１５を削除する。

【０２５２】また、種々の方式で圧縮等されたデータ（あるいは復号の必要ないデータ）のいずれも出力できるように、複数種類のデコード回路等を設け、これを適宜切替て使用し（あるいはこれらを使用しないように）構成することも可能である。この場合、例えば、ＤＶＤ等の記録媒体から使用すべきデコード等を示す識別子を読み込む、この識別子に従って適切なデコード回路等を選択等する方法が考えられる。

【０２５３】第２の実施形態および第３の実施形態にて示した図６の鍵判定回路１２０の構成は一例であり、この他にも種々の構成が考えられる。

【０２５４】さらに、鍵判定用情報としてE_{SK}（S_K）を用いる構成は、この他にも種々のものが考えられる。

例えば、鍵判定に用いる情報としてD_{SK}（S_K）を用い、鍵判定回路１２０では、ＤＶＤ等の記録媒体から読み込んだE_{Mki}（S_K）を記憶されたマスターキーM_{kj}で復号してS_{kij}＝D_{Mkj}（E_{Mki}（S_K））を得て、このS_{kij}をS_{kij}自身で復号してS_K'''＝D_{Skij}（S_{kij}）を得て、次に、このS_K''とＤＶＤ等の記録媒体から読み込んだD_{SK}（S_K）を比較し、一致した場合、第１のセッションキーS_K＝S_{kij}は正しいものと判定して出力する。

【０２５５】また、鍵判定用情報の他の例として、２回以上暗号化または復号を行ったもの、例えば、E_{SK}（E_{SK}（S_K））、D_{SK}（D_{SK}（S_K））、あるいは各E_{Mki}（S_K）に対応してE_{Mki}（E_{Mki}（S_K））を設けるものなど種々のものが考えられる。

【０２５６】また、各実施形態では、鍵判定用情報をもとに（方法１）～（方法５）で示した手順を用いて、復号により得られた鍵が第１のセッションキーが正しいものであることを判定したが、ＤＶＤ等の記録媒体にｉの順番ですべてのE_{Mki}（S_K）を記録しておき、復号ユニットにはｉとM_{ki}を対応付けて登録しておくことにより、鍵判定用情報、鍵判定手順、そのための構成を省略することができる。なお、あるｉについてのM_{ki}が使用不可となった場合には、ＤＶＤ等の記録媒体にE_{Mki}（S_K）の代わりに無効を示す情報を格納するのが望ましい。

【０２５７】次に、図１１を参照しながら、ＤＶＤ－ＲＯＭを例に取り上げ、上記した第３の実施形態を用いたディスクメーカ（映画、音楽等の著作物のＤＶＤを制作するメーカとする）とプレーヤメーカ（単体のＤＶＤプレーヤのメーカとする）とマスターキーを管理する鍵管理組織による鍵の管理方法等について説明する。なお、Ｄａｔａは、コンテンツの他に、前述したように鍵情報である場合もある（Ｄａｔａが鍵情報S_{kt}である場合のこの鍵情報S_{kt}を用いた暗号化や復号等についての説明は省略する）。なお、図１１において、処理等に用いる計算機等については省略してある。

【０２５８】また、図１２には暗号化のためのシステムに関して説明するための図を示す。図１２の暗号化回路３０１，３１２，３０３は、同一の装置（計算機等）上に搭載される場合と、異なる装置（計算機等）上に搭載される場合があり、後者の場合には、装置間で情報の受け渡しが行われる。また、暗号化回路３０１，３１２，３０３は、ハードウェアで構成することも、ソフトウェアで構成することも可能である。

【０２５９】ここでは、上記した（方法３）のＤＶＤにはｉ＝１～ｎのすべてに対応するｎ個のマスターキーE_{MKi}（S_K）を記録し、ＤＶＤプレーヤ（復号化ユニット１１４ｂ）内にはｊを１～ｎのうちのから予め選択されたｍ（２＜ｍ＜ｎ）種類のものとするｍ個のマスターキーM_{kj}を備える場合について説明する。なお、ＤＶＤ

41

プレーヤメーカにはマスターキーMkjを排他的に割り当てるものとする。また、ここでは、ｎ＝１００、ｍ＝１０とする。

【０２６０】また、ここでは、鍵判定用情報として、ＤＶＤにはEsk（Sk）を記録する方法を用いるものとする（図１２の３０２の部分は、鍵判定用情報をEsk（Sk）とした場合のものである）。

【０２６１】まず、鍵管理組織２００では、マスターキーMki（ｉ＝１～１００）を保管している。マスターキーに数は、プレーヤメーカの新規参入や破られた場合の予備等のために、余分に設定しておくのが望ましい。

【０２６２】鍵管理組織２００では、各プレーヤメーカ２０１～２０３に、排他的にマスターキーMki（ｉ＝１～１００）を割り当てる。例えば、図１１のように、プレーヤメーカAにマスターキーMki（ｉ＝１０～１９）を、プレーヤメーカBにマスターキーMki（ｉ＝２０～２９）を、プレーヤメーカCにマスターキーMki（ｉ＝３０～３９）を割り当てる。鍵管理組織２００（の計算機等）から各プレーヤメーカ（の計算機等）には、割り当てたマスターキーを通信媒体あるいは記録媒体等により送付する。その際、暗号通信等を用いて安全に受け渡しするのが望ましい。

【０２６３】各プレーヤメーカは、個別に、鍵管理組織２００から割り当てられたマスターキーを管理する。そして、各プレーヤメーカは、この割り当てられたマスターキーを用いて、第３の実施形態で示したような構成を有するＤＶＤプレーヤを製造して販売する。

【０２６４】一方、ここでは、鍵管理組織２００からディスクメーカ２２１～２２３へは、マスターキーのプレインデータは渡さないようにするものとする。

【０２６５】まず、各ディスクメーカ（ａとする）は、自身で第１のセッションキーSk を決め（例えばディスク毎に決め）、第１のセッションキーSk を鍵管理組織２００に渡す。鍵管理組織２００は、受け取った第１のセッションキーSk を全てのマスターキーMki（ｉ＝１～１００）でそれぞれ暗号化してEmki（Sk）、（ｉ＝１～１００）を得る（図１２の暗号化回路３０１を用いる）。そして、鍵管理組織２００は、Emki（Sk）、（ｉ＝１～１００）を、ディスクメーカａに渡す。

【０２６６】鍵管理組織２００（の計算機等）とディスクメーカ（の計算機等）との間での情報の受け渡しも、上記と同様に、割り当てたマスターキーを通信媒体あるいは記録媒体等にて暗号通信等を用いて安全に行うのが望ましい。

【０２６７】ディスクメーカａでは、Emki（Sk）、（ｉ＝１～１００）と、Esk（Sk）と、Esk（Ｄａｔａ））とをＤＶＤ２３１に記録して販売する。なお、Sk 自身でSk を暗号化してEsk（Sk）を得る操作は、ディスクメーカ側で行う方法と、マスターキーによる暗

42

号化と同様に鍵管理組織２００側で行う方法とがある（図１２の暗号化回路３１２を用いる）。また、少なくとも、コンテンツの暗号化はディスクメーカにて行うものとする（図１２の暗号化回路３０３を用いる）。

【０２６８】ディスクメーカａでは、例えば、Sk について、受け取ったEmki（Sk）と鍵判定用情報であるEsk（Sk）とEsk（Ｄａｔａ）（あるいはＤａｔａ）について管理する。

【０２６９】他のディスクメーカについても同様である。

【０２７０】なお、万一、マスターキーが破られたことが発覚した場合、それ以降、その破られたマスターキーを用いずに、ＤＶＤを制作するようにする。例えば、ｉ＝１９のマスターキーが破られた場合、ＤＶＤには、ｉ＝１～１８、２０～１００の９９個に対応するEmki（Sk）が記録される。

【０２７１】また、マスターキーが破られたことが発覚した場合、それ以降、その破られたマスターキーが割り当てられているプレーヤメーカでは、これを除いてＤＶＤプレーヤを製造して販売するようにするのが望ましい。例えば、ｉ＝１９のマスターキーが破られた場合、プレーヤメーカAは、ｉ＝１０～１８のマスターキーを用いてＤＶＤプレーヤを製造して販売する。

【０２７２】また、既に販売されたｉ＝１９のマスターキーを持つてＤＶＤプレーヤについては、そのまま使用しても構わない。ただし、ユニット交換等によってｉ＝１９のマスターキーを持たないようにしてもよい。

【０２７３】従って、マスターキーを安全かつ有効に管理できるとともに、不正なマスターキー解読に対するリスクを分散し、マスターキー解読後も上記システムが安全かつ有効に機能するようにすることができる。

【０２７４】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０２７５】

【発明の効果】本発明によれば、複数の第２の鍵のうちの少なくとも１つを持つ正当なもののみが、第１の鍵を得ることができ、従って第１の鍵で暗号化されたデータのプレインデータを得ることができる。

【０２７６】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るシステムの構成を示すブロック図

【図２】同実施形態の動作を示すフローチャート

【図３】記録媒体に暗号化された鍵と暗号化されたデータを格納する形式の一例を示す図

【図４】ＣＰＵ　ＢＵＳからデータを保存した場合について説明するための図

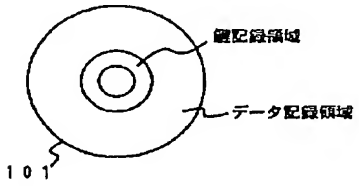
43

【図５】本発明の第２の実施形態に係るシステムの構成を示すブロック図
【図６】鍵判定部の内部構成の例を示す図
【図７】同実施形態の動作を示すフローチャート
【図８】同実施形態の動作を示すフローチャート
【図９】本発明の第３の実施形態に係るシステムの構成を示すブロック図
【図１０】同実施形態の動作を示すフローチャート
【図１１】鍵の管理方法について説明するための図
【図１２】暗号化について説明するための図
【符号の説明】
１０１…ＤＶＤ
１０２，２０２…マスターキーを用いて暗号化された第１のセッションキー
１０３，２０３…第１のセッションキーを用いて暗号化された画像データ
１０４…暗号化回路
１０５…マスターキー
１０６…第２のセッションキー
１０７…暗号化ユニット
１０８…マスターキーを用いて復号された第２のセッションキー

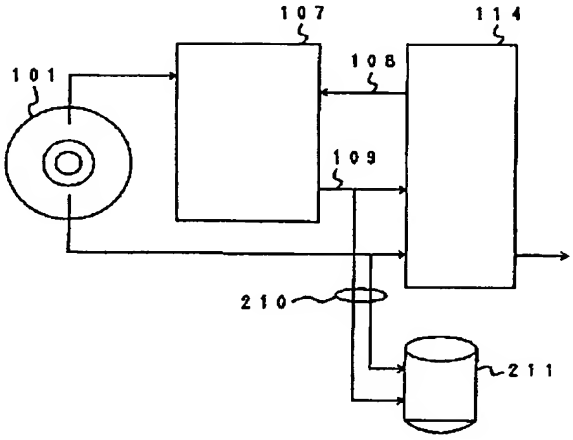
44

１０９…第２のセッションキーを用いて暗号化された、マスターキーを用いて暗号化された第１のセッションキー
１１０…ＣＰＵ　ＢＵＳ
１１１…セッションキー生成回路
１１２…復号化回路
１１３…第１のセッションキー
１１４，１１４ａ，１１４ｂ…復号化ユニット
１１５…ＭＰＥＧデコーダ回路
１１６…ディジタル／アナログ変換回路
２０９…ＤＶＤの読み出し出力から別の媒体にコピーするための線
２１０…ＣＰＵ　ＢＵＳから別の媒体にコピーするための線
２１１…ディジタル記憶媒体
２００…鍵管理組織
２０１～２０３…プレーヤメーカ
２２１～２２３…ディスクメーカ
２３１～２３３…ＤＶＤ
３０１，３１２，３０３…暗号化回路

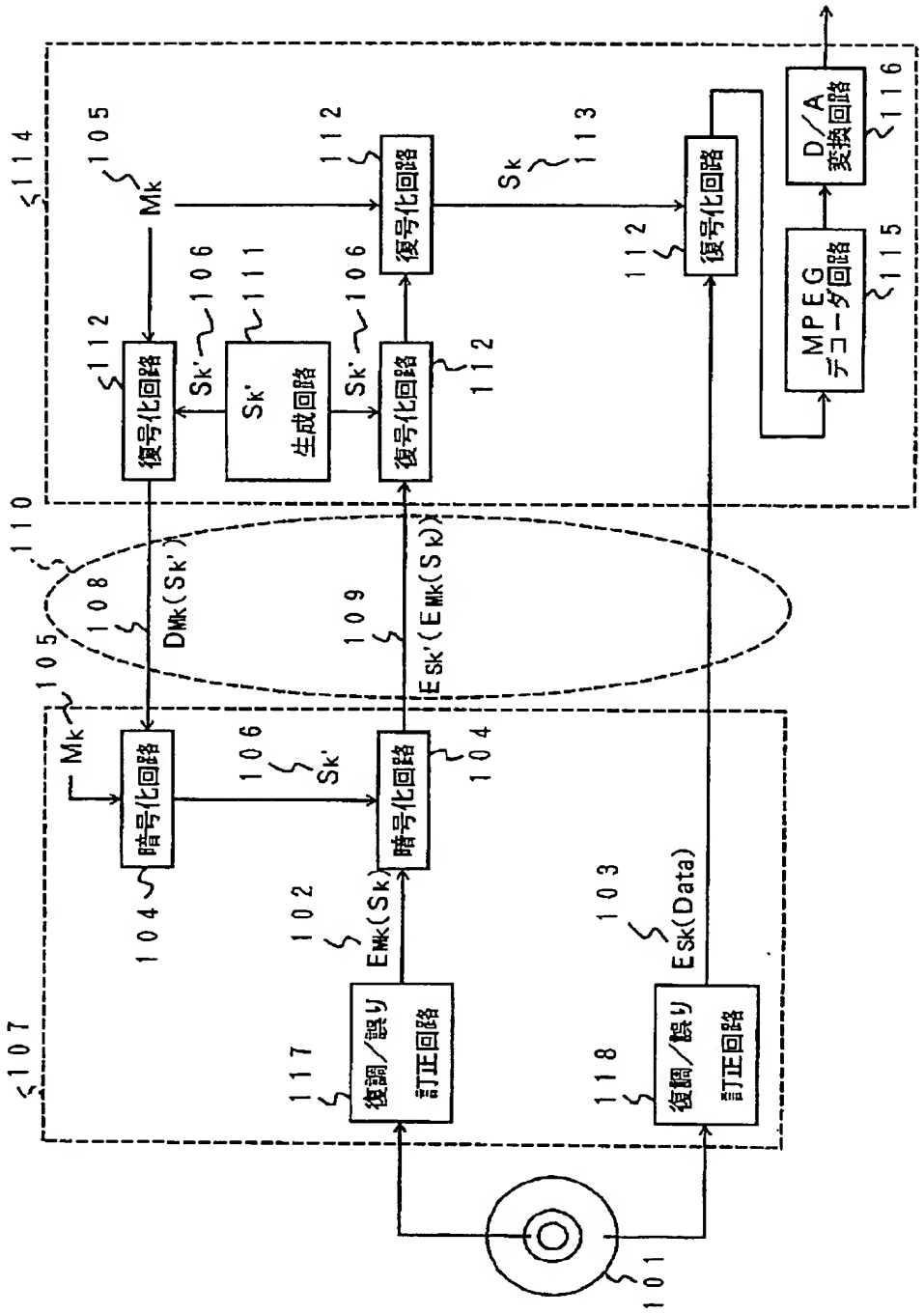
【図３】



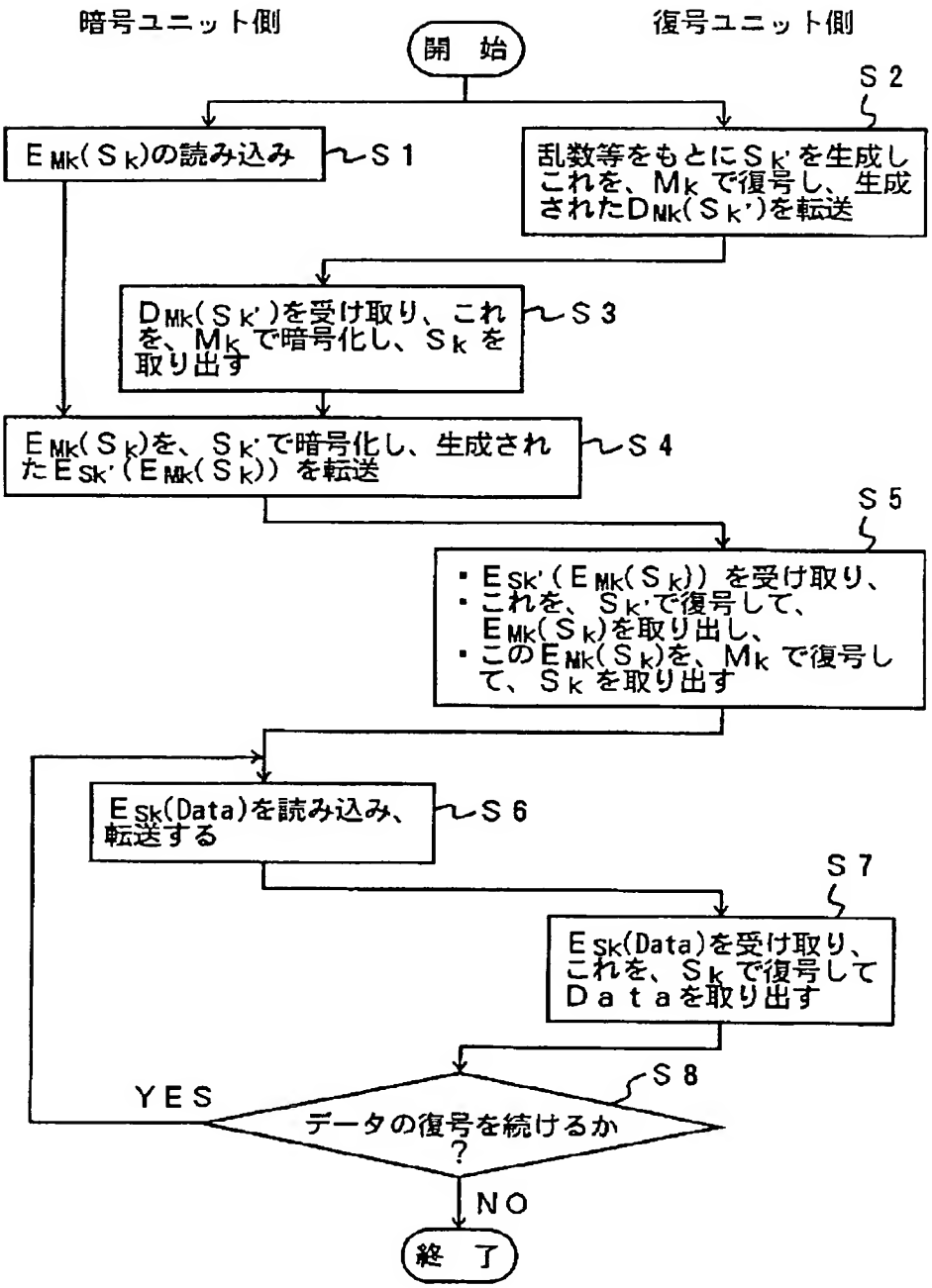
【図４】



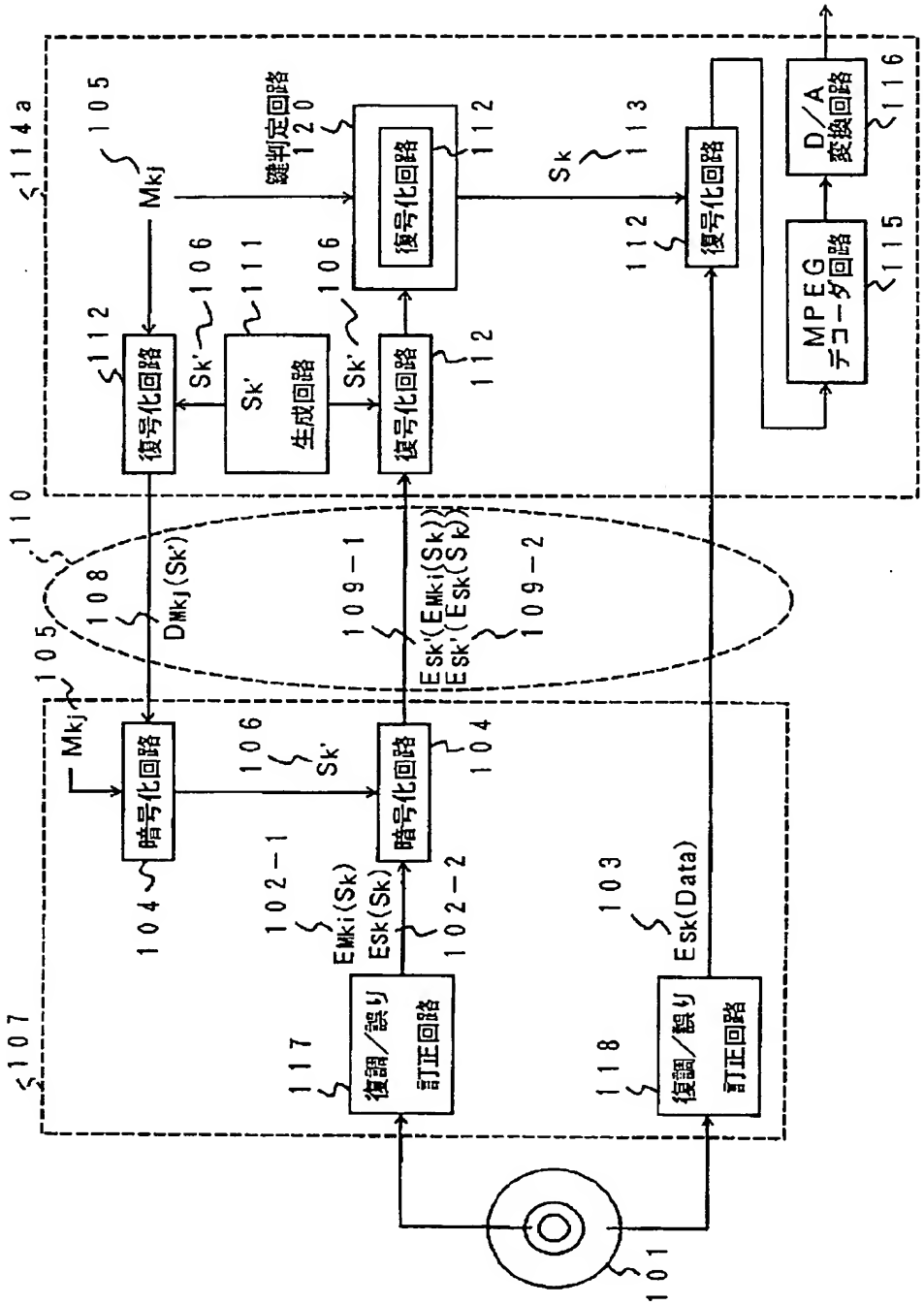
【図１】


114
105
Mk
112
復号化回路
106
Sk'
111
Sk'
生成回路
106
Sk'
112
復号化回路
112
復号化回路
Sk
113
D/A
変換回路
116
MPEG
デコーダ回路
115
110
108
DMk(Sk')
109
ESk'(EMk(SK))
105
Mk
104
暗号化回路
106
Sk'
104
暗号化回路
102
EMk(Sk)
103
ESk(Data)
107
117
復調/誤り
訂正回路
118
復調/誤り
訂正回路
101

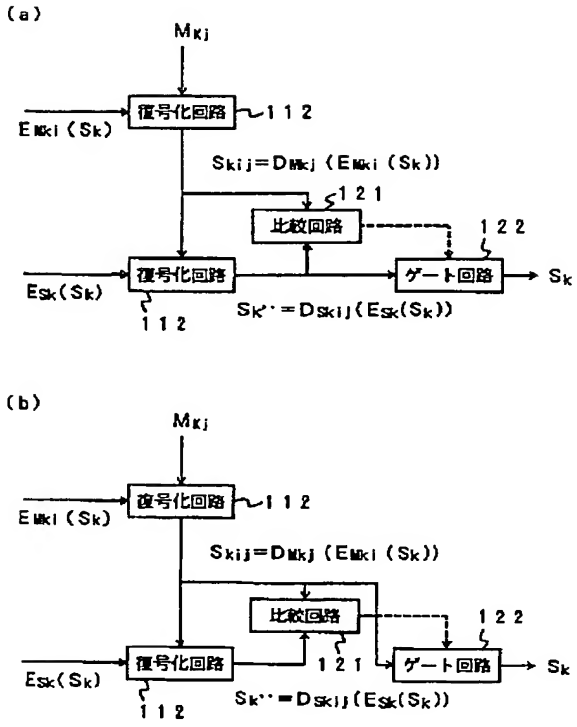
【図２】


暗号ユニット側
復号ユニット側
開　始
S２
E Mk(S k)の読み込み
S１
乱数等をもとにS k'を生成し これを、Mk で復号し、生成 されたD Mk(S k')を転送
D Mk(S k')を受け取り、これ を、Mk で暗号化し、S k を 取り出す
S３
E Mk(S k)を、S k'で暗号化し、生成され たE Sk'(E Mk(S k)) を転送
S４
S５
・E Sk'(E Mk(S k)) を受け取り、
・これを、S k'で復号して、 E Mk(S k)を取り出し、
・この E Mk(S k)を、Mk で復号し て、S k を取り出す
E Sk(Data)を読み込み、 転送する
S６
S７
E Sk(Data)を受け取り、 これを、S k で復号して Ｄａｔａを取り出す
S８
YES
データの復号を続けるか ?
NO
終　了

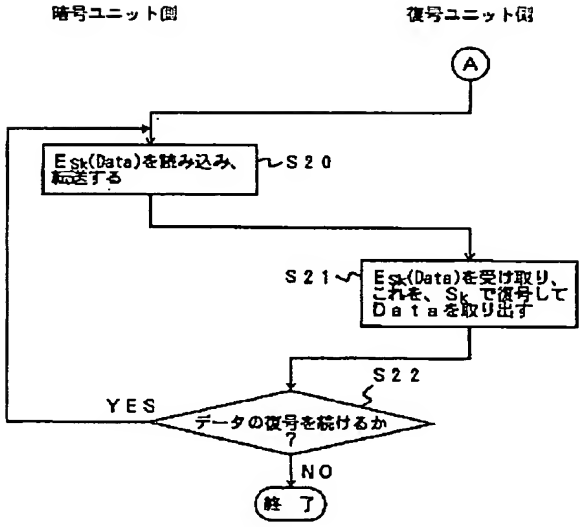
【図５】


114a
105
Mkj
鍵判定回路
120
112
復号化回路
113
Sk
D/A
変換回路
116
106
Sk'
111
Sk'
生成回路
106
Sk'
112
復号化回路
112
復号化回路
MPEG
デコーダ回路
115
110
108
Dmkj(Sk')
109-1
Emki(Sk)
Esk(Sk)
109-2
Esk'(Emki(Sk))
Esk'(Esk(Sk))
105
Mkj
暗号化回路
106
Sk'
暗号化回路
104
104
102-1
Emki(Sk)
Esk(Sk)
102-2
103
Esk(Data)
107
117
復調/誤り
訂正回路
118
復調/誤り
訂正回路
101

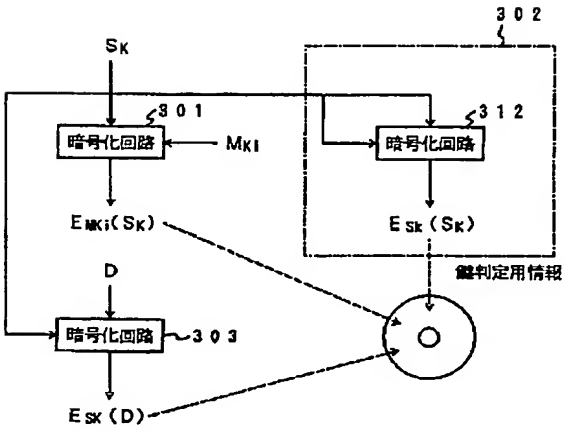
【図６】


(a)
Mkj
復号化回路
112
Emki(Sk)
Skij=Dmkj(Emki(Sk))
121
比較回路
122
復号化回路
ゲート回路
Sk
Esk(Sk)
112
Sk''=Dskij(Esk(Sk))
(b)
Mkj
復号化回路
112
Emki(Sk)
Skij=Dmkj(Emki(Sk))
比較回路
122
復号化回路
121
ゲート回路
Sk
Esk(Sk)
112
Sk''=Dskij(Esk(Sk))

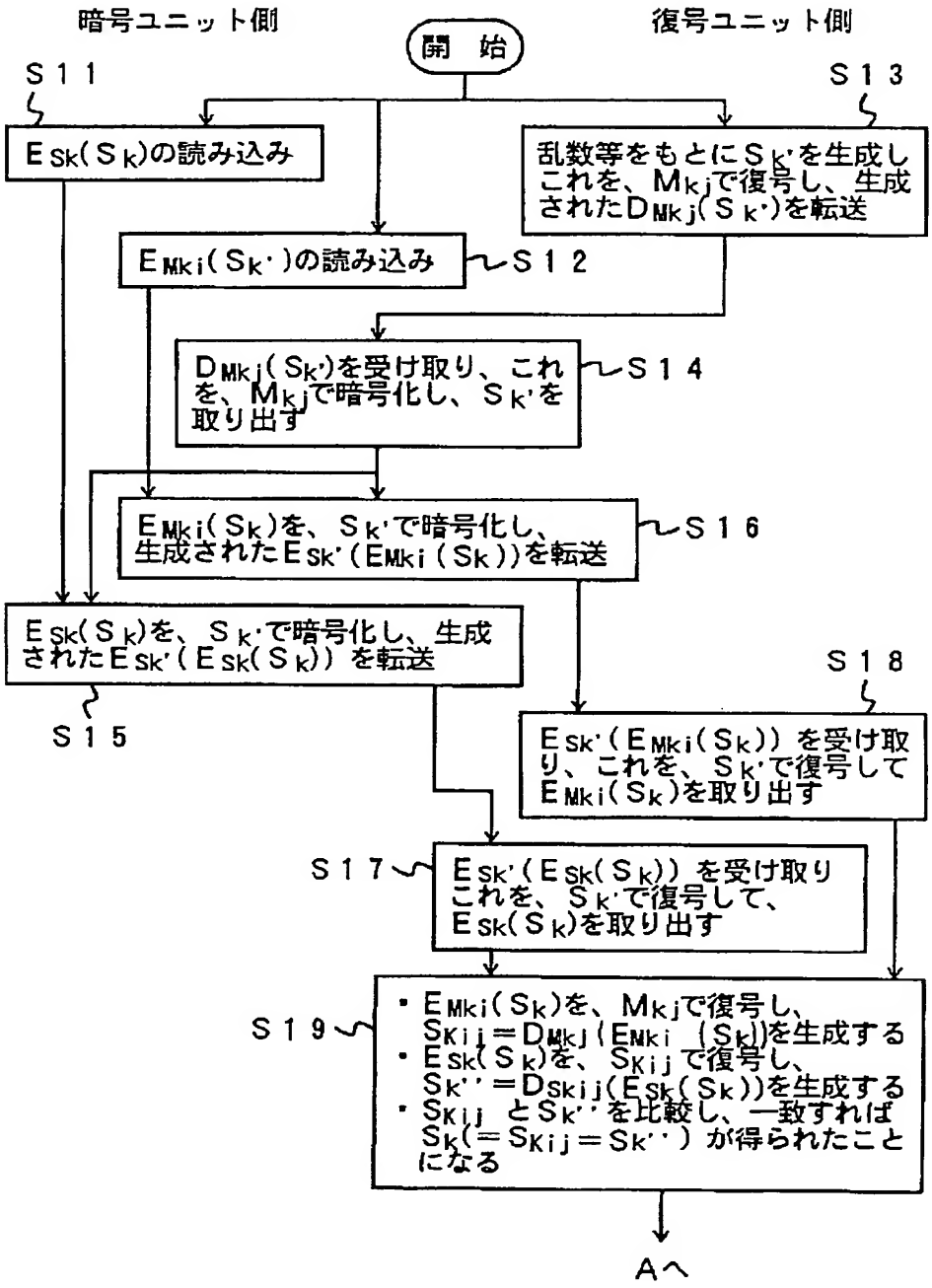
【図８】


暗号ユニット側
復号ユニット側
A
Esk(Data)を読み込み、転送する
S20
S21
Esk(Data)を受け取り、これを、Sk で復号してDataを取り出す
S22
YES
データの復号を続けるか
NO
終了

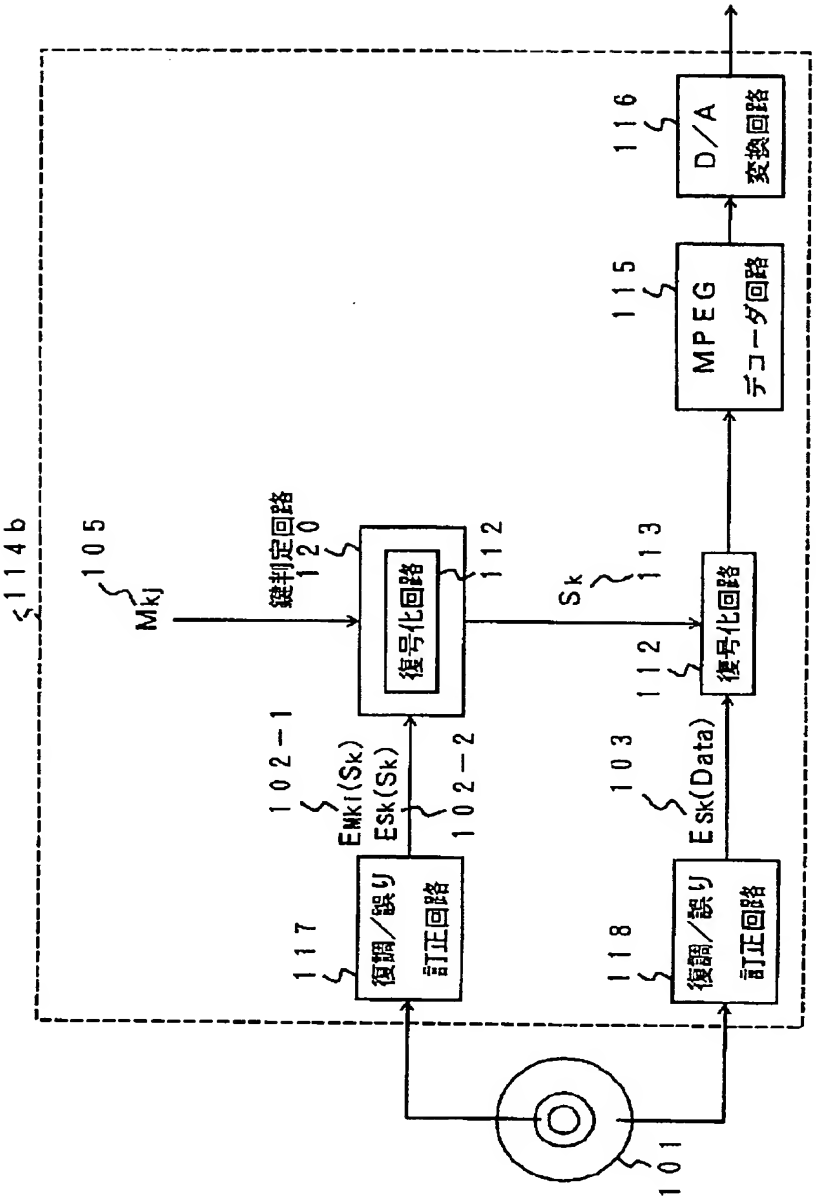
【図１２】


302
Sk
301
312
暗号化回路
Mki
暗号化回路
Emki(Sk)
Esk(Sk)
D
鍵判定用情報
暗号化回路
303
Esk(D)

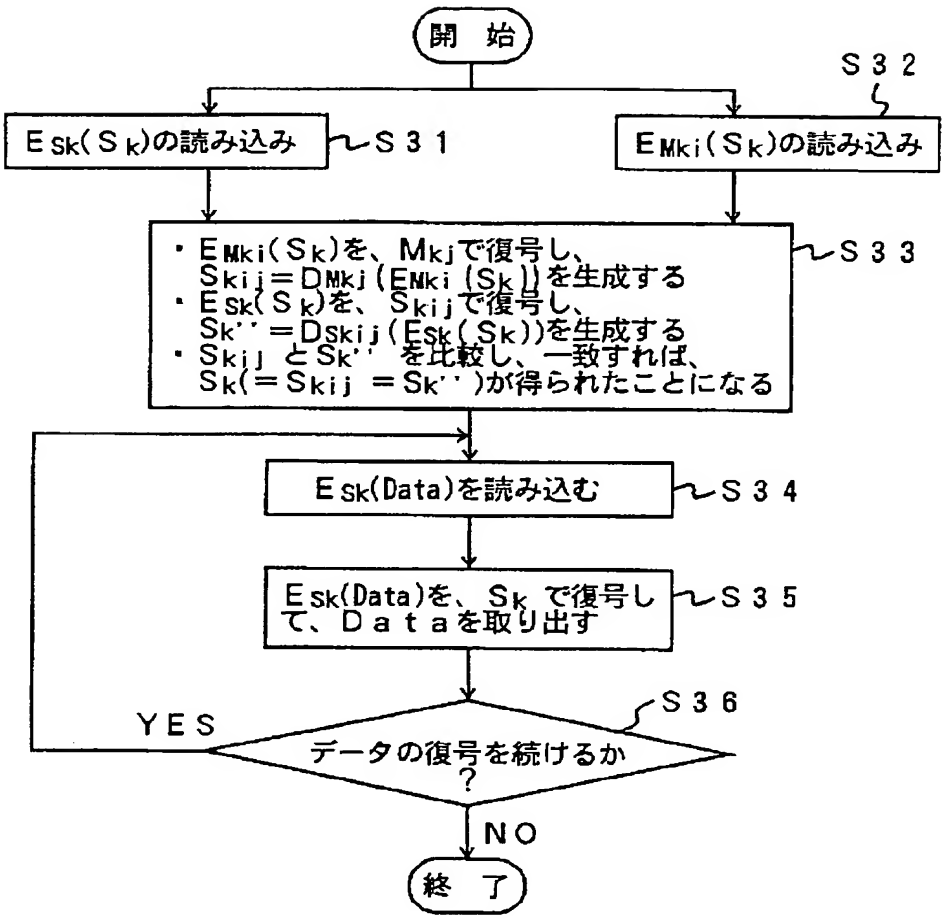
【図７】


暗号ユニット側
復号ユニット側
開　始
Ｓ１１
Ｓ１３
Ｅ Sk(Ｓ k)の読み込み
乱数等をもとにＳ k'を生成し
これを、Ｍ kjで復号し、生成
されたＤ Mkj(Ｓ k')を転送
Ｅ Mki(Sk')の読み込み
Ｓ１２
Ｄ Mkj(Sk')を受け取り、これ
を、Ｍ kjで暗号化し、Ｓ k'を
取り出す
Ｓ１４
Ｅ Mki(Ｓ k)を、Ｓ k'で暗号化し、
生成されたＥ Sk'(Ｅ Mki (Ｓ k))を転送
Ｓ１６
Ｅ Sk(Ｓ k)を、Ｓ k'で暗号化し、生成
されたＥ Sk'(Ｅ Sk(Ｓ k)) を転送
Ｓ１５
Ｓ１８
Ｅ Sk'(Ｅ Mki(Ｓ k)) を受け取
り、これを、Ｓ k'で復号して
Ｅ Mki(Ｓ k)を取り出す
Ｓ１７
Ｅ Sk'(Ｅ Sk(Ｓ k)) を受け取り
これを、Ｓ k'で復号して、
Ｅ Sk(Ｓ k)を取り出す
Ｓ１９
・Ｅ Mki(Ｓ k)を、Ｍ kjで復号し、
Ｓ Kij＝Ｄ Mkj(Ｅ Mki (Ｓ k))を生成する
・Ｅ Sk(Ｓ k)を、Ｓ Kijで復号し、
Ｓ k''＝Ｄ Skij(Ｅ Sk(Ｓ k))を生成する
・Ｓ Kij とＳ k''を比較し、一致すれば
Ｓ k(＝Ｓ Kij＝Ｓ k'') が得られたこと
になる
Aへ

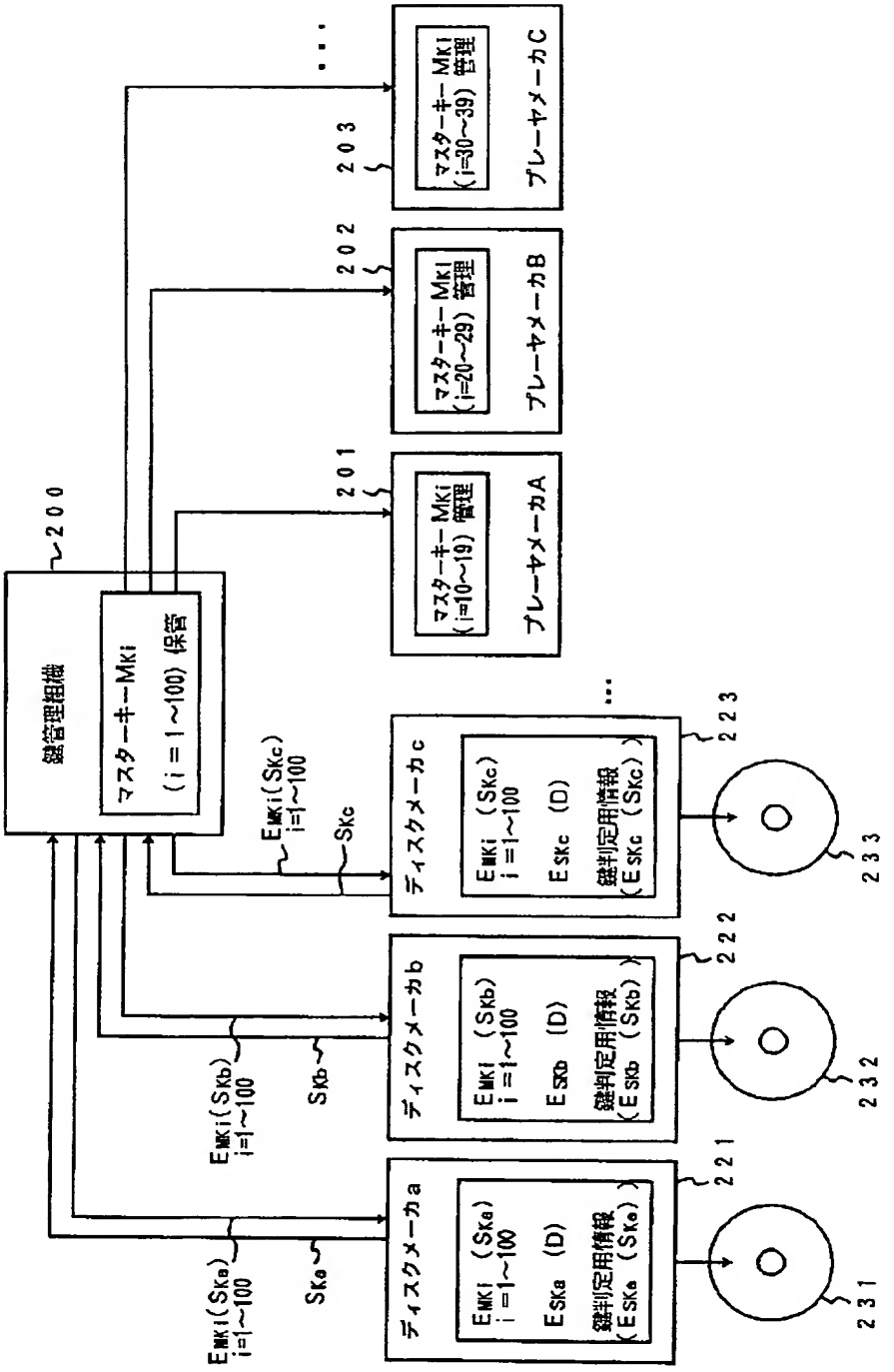
【図９】


114b
105
Mkj
鍵判定回路
120
復号化回路
112
Sk
113
復号化回路
112
MPEG
デコーダ回路
115
D/A
変換回路
116
102-1
EMki(Sk)
Esk(Sk)
102-2
103
Esk(Data)
復調/誤り
訂正回路
117
復調/誤り
訂正回路
118
101

【図１０】


開　始
S３２
ESk(Sk)の読み込み
S３１
EMki(Sk)の読み込み
・EMki(Sk)を、Mkjで復号し、
Skij＝DMkj(EMki(Sk))を生成する
・ESk(Sk)を、Skijで復号し、
Sk''＝DSkij(ESk(Sk))を生成する
・Skij とSk'' を比較し、一致すれば、
Sk(＝Skij ＝Sk'')が得られたことになる
S３３
ESk(Data)を読み込む
S３４
ESk(Data)を、Sk で復号して、Ｄａｔａを取り出す
S３５
S３６
YES
データの復号を続けるか？
NO
終　了

【図１１】



フロントページの続き

(51) Int. Cl.[6]	識別記号	FI	
		H04L 9/00	601E
			601B

(72)発明者　小島　正
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

(72)発明者　平山　康一
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内